bitdefender
ANTIVIRUS PLUS v10

10th anniversary

Manual do Utilizador

Antivírus

Firewall

Antispam

Antispyware

bitdefender
secure your every bit

Copyright© 2007 SOFTWIN

BitDefender Antivirus Plus v10

Manual do Utilizador

BitDefender

Publicado 2007.03.13
Version 10.2

Copyright© 2007 SOFTWIN

Aviso Legal

Todos os direitos reservados. Nenhuma parte deste livro pode ser reproduzida ou transmitida de qualquer forma ou por quaisquer meios, electrónicos ou mecânicos, incluindo fotocópias, gravação, ou qualquer sistema de arquivo de informação, sem a permissão por escrito de um representante autorizado de SOFTWIN. A inclusão de pequenas frases do texto em comparativas poderão ser feitas desde que seja feita a menção da fonte da frase em questão. O conteúdo não pode ser de forma alguma modificado.

Aviso e Renúncia. Este produto e a sua documentação estão protegidas por direitos de autor. A informação neste documento é apresentada numa base de "tal como é", sem qualquer garantia. Apesar de todas as precauções terem sido tomadas na preparação deste documento, os autores não serão responsabilizados por qualquer pessoa ou entidade com respeito a qualquer perda ou dano causado ou alegadamente causado directa ou indirectamente pela informação contida neste livro.

Este livro contém links para Websites de terceiras partes que não estão baixo controlo da SOFTWIN, e a SOFTWIN não é responsável pelo conteúdo de qualquer site acedido por link. Se aceder a um site de terceiras partes mencionado neste manual, faz isso à sua própria conta e risco. A SOFTWIN fornece esses links apenas para facilitar, e a inclusão do link não implica que a SOFTWIN endosse ou aceite qualquer responsabilidade pelo conteúdo deste sites de terceiras partes.

Marcas Registadas. Nomes de Marcas Registadas poderão aparecer neste livro. Todas as marcas registadas ou não registadas neste documento são da exclusiva propriedade dos seus respectivos proprietários.

bitdefender
secure your every bit

Índice

Licença e garantia ..... **ix**

Prefácio ..... **xiii**

1. Convenções Usadas neste Manual xiii
   1.1. Convenções Tipográficas xiii
   1.2. Avisos xiv
2. A estrutura do Manual xiv
3. Pedido de Comentários xv

Acerca do BitDefender 1

1. Quem é BitDefender? **3**
   1.1. Porquê BitDefender? 3

Instalação do Produto 7

2. Instalação de BitDefender Antivirus Plus v10 ..... **9**
   2.1. Requisitos do Sistema 9
   2.2. Passos da Instalação 10
   2.3. Assistente Inicial de Instalação 12
      2.3.1. Passo 1/8 - Assistente Inicial de Instalação BitDefender 13
      2.3.2. Passo 2/8 - Registar BitDefender Antivirus Plus v10. 13
      2.3.3. Passo 3/8 - Criar uma conta BitDefender 14
      2.3.4. Passo 4/8 - Inserir Detalhes da Conta 15
      2.3.5. Passo 5/8 - Aprenda acerca de RVTR 16
      2.3.6. Passo 6/8 – Seleccionar as Tarefas a Serem Executadas 16
      2.3.7. Passo 7/8 - Esperar que as Tarefas Terminem 17
      2.3.8. Passo 8/9 - Ver Resumo 18
   2.4. Upgrade (Mudança de versão) 18
   2.5. Remover, Reparar ou Modificar o BitDefender 19

Descrição e Características 21

3. BitDefender Antivirus Plus v10 ..... **23**
   3.1. Antivírus 23
   3.2. Firewall Aplicacional 24
   3.3. Antispam 24
   3.4. Antispyware 25
   3.5. Outras Características 25

4. Módulos BitDefender **27**
   4.1. Módulo Geral 27
   4.2. Módulo Antivírus 27

4.3. Módulo Firewall 27
4.4. Módulo Antispam 28
4.4.1. Esquema de funcionamento 28
4.4.2. Filtros Antispam 29
4.5. Módulo Antispyware 32
4.6. Módulo de Actualização 32

Consola de Administração 35

5. Geral 37
5.1. Área de Notificação 38
5.2. Barra de Actividade da Análise 39

6. Módulo Geral 41
6.1. Administração Central 42
6.1.1. Tarefas Rápidas 42
6.1.2. Nível de Segurança 43
6.1.3. Estado do Registo 44
6.2. Configurações da Consola de Administração 45
6.2.1. Configurações Gerais 45
6.2.2. Configurações do Relatório de Vírus 46
6.2.3. Configurações da Máscara 47
6.2.4. Configurações de Administração 47
6.3. Eventos 48
6.4. Registo do produto 49
6.4.1. Assistente de Registo 49
6.5. Acerca 54

7. Módulo Antivírus 55
7.1. Análise No-acesso 55
7.1.1. Nível de Protecção 56
7.2. Análise A-pedido 61
7.2.1. Tarefas de Análise 61
7.2.2. Menú de Atalho 63
7.2.3. Propriedades da Tarefa de Análise 63
7.2.4. Tipos de Análise A-pedido 73
7.2.5. Análise de Rootkits 78
7.3. Quarentena 79

8. Módulo Firewall 83
8.1. Estado da Firewall 83
8.1.1. Nível de Protecção 84
8.2. Controlo de Tráfego 85
8.2.1. Adicionar Regras Automaticamente 86
8.2.2. Adicionar Regras Manualmente 86

9. Módulo Antispam 93
9.1. Estado do Antispam 93

9.1.1. Preencher a Lista de Endereços 94
9.1.2. Definir o Nível de Tolerância 97
9.2. Configurações de Antispam 99
9.2.1. Configurações de Antispam 99
9.2.2. Filtros Antispam Básicos 100
9.2.3. Filtros Antispam Avançados 100
9.3. Integração como o Microsoft Outlook / Outlook Express / Windows Mail 101
9.3.1. Barra de Ferramentas do Antispam 101
9.3.2. Assistente de Configuração Antispam 108

10. Módulo Antispyware 115
10.1. Estado do Antispyware 116
10.1.1. Nível de Protecção 117
10.2. Configuração Avançada - Controlo de Privacidade 117
10.2.1. Assistente de Configuração 118
10.2.2. Gerindo as Regras 121
10.3. Configuração Avançada - Controlo de registo 122
10.4. Configuração Avançada - Controlo de Ligação 123
10.4.1. Assistente de Configuração 125
10.5. Configuração Avançada - Controlo de Cookies 127
10.5.1. Assistente de Configuração 129
10.6. Configuração Avançada - Controlo de Script 130
10.6.1. Assistente de Configuração 131
10.7. Info do Sistema 133

11. Módulo de Actualização 135
11.1. Actualização Automática 135
11.2. Actualização Manual 136
11.2.1. Actualização Manual com o ficheiro `weekly.exe` 137
11.2.2. Actualização Manual com os `arquivos zip` 137
11.3. Definições de actualização 139
11.3.1. Configuração para a Localização das Actualizações 140
11.3.2. Opções de Actualização Automática 140
11.3.3. Configuração da Actualização Manual 141
11.3.4. Opções Avançadas 141

Dicas de Utilização 143

12. Dicas de Utilização 145
12.1. Como Proteger o seu Computador Ligado À Internet 145
12.2. Como Proteger o Seu Computador contra as Ameaças de Malware 146
12.3. Como Configurar uma Tarefa de Análise 147
12.4. Como Manter o seu Computador Livre de Spam 148

CD de Emergência BitDefender 151

13. Geral 153

13.1. O que é o KNOPPIX? 153
13.2. Requisitos do Sistema 153
13.3. Software incluído 154
13.4. BitDefender Linux Security Solutions 154
13.4.1. BitDefender SMTP Proxy 154
13.4.2. BitDefender Remote Admin 155
13.4.3. BitDefender Linux Edition 155

14. LinuxDefender Howto 157
14.1. Iniciar e Parar 157
14.1.1. Iniciar LinuxDefender 157
14.1.2. Stop LinuxDefender 158
14.2. Configurar a Ligação à Internet 159
14.3. Actualização BitDefender 160
14.4. Análise de Vírus 160
14.4.1. Como posso aceder aos meus dados no Windows? 160
14.4.2. Como posso levar a cabo uma análise completa ao sistema? 161
14.5. Construir um Instant Mail Filtering Toaster 162
14.5.1. Pré-requisitos 162
14.5.2. O e-mail toaster 162
14.6. Perform a Network Security Audit 163
14.6.1. Analisar em busca de Rootkits 163
14.6.2. Nessus - the Network Scanner 164
14.7. Verifique o Estado da RAM do Seu Sistema 164

Obter Ajuda 167

15. Suporte 169
15.1. Departamento de Suporte 169
15.2. Ajuda On-line 169
15.2.1. BitDefender Knowledge Base 169
15.3. Informação de Contacto 170
15.3.1. Endereços Web 170
15.3.2. Escritórios 170

Glossário 173

Licença e garantia

SE NÃO CONCORDA COM ESTES TERMOS E CONDIÇÕES NÃO INSTALE O SOFTWARE. AO SELECCIONAR "EU ACEITO", "OK", "CONTINUAR", "SIM" OU AO INSTALAR E USAR O SOFTWARE DE QUALQUER FORMA, ESTÁ A AFIRMAR QUE COMPREENDEU COMPLETAMENTE E ACEITOU OS TERMOS DE ESTE ACORDO.

Estes termos abrangem as Soluções e Serviços BitDefender para utilizadores individuais que lhe foram licenciadas, incluindo documentação relacionada, updates (actualizações da base de vírus) e upgrades (mudanças de versão) das aplicações que lhe foram entregues como parte da licença adquirida ou qualquer acordo de serviço tal como definido na documentação ou em qualquer cópia desses itens.

Este Acordo da Licença é um acordo legal entre você (seja um indivíduo ou representante legal) e a SOFTWIN para uso do produto de software SOFTWIN acima identificado, o qual inclui software de computador e serviços e poderá incluir meios associados, materiais impressos, e documentação "online" ou electrónica (daqui em diante designado por "BitDefender"), todos os quais estão protegidos pelos pelas leis internacionais dos direitos de autor e tratados internacionais. Ao instalar, copiar, ou usar de outra forma o BitDefender, estará a concordar com os termos deste acordo.

Se não concorda com os termos deste acordo, não instale ou use o BitDefender.

Licença BitDefender. O BitDefender está protegido pelas leis dos direitos de autor e pelos tratados internacionais sobre direitos de autor, como também por outras leis e tratados intelectuais de propriedade. O BitDefender é licenciado, não é vendido.

CONCESSÃO DE LICENÇA. Pela presente, a SOFTWIN concede-lhe a si, e apenas a si a seguinte licença não-exclusiva, limitada, não-transmissível e passível de royaltie para utilizar o BitDefender.

SOFTWARE APLICAÇÃO. Pode instalar e usar BitDefender, em tantos computadores quantos os abrangidos pelo número total de licenças de utilizador. Pode fazer uma cópia adicional para efeitos de back-up (cópia de segurança).

LICENÇA DE UTILIZADOR DE COMPUTADOR INDIVIDUAL. Esta licença aplica-se ao software BitDefender que pode ser instalado num único computador que não providencie serviços de rede. O utilizador primário pode instalar este software num único computador e fazer uma cópia adicional num dispositivo distinto para efeitos de backup. O número de utilizadores primários permitidos corresponde ao número de utilizadores abrangidos pela licença.

TERMOS DE LICENÇA. A Licença aqui outorgada começa na data da aquisição do BitDefender e expira no final do período para o qual a licença foi adquirida.

UPGRADES. Se o BitDefender estiver marcado como um upgrade (mudança de versão), tem de estar correctamente licenciado para usar um produto identificado pela SOFTWIN como sendo elegível para o upgrade para poder usar o BitDefender. O BitDefender marcado como upgrade substitui e/ou suplementa o produto que forma as bases para a sua elegibilidade de upgrade. Pode utilizar o produto resultante do upgrade apenas nos termos deste Acordo de Licença. Se o BitDefender for um upgrade de um componente de um pacote de programas de software que licenciou como um único produto, o BitDefender pode ser usado e transferido apenas como uma parte desse único pacote de produtos, e não pode ser separado para uso por mais do que o número total de utilizadores licenciados. Os termos e condições desta licença substituem quaisquer acordos prévios que possam ter existido entre si e a SOFTWIN com respeito ao produto original ou ao upgrade resultante.

DIREITOS DE AUTOR. Todos os direitos, títulos e interesses no e para o BitDefender e todos os direitos de autor em e no BitDefender (incluindo mas não limitado a qualquer imagem, fotografias, acessos, animações, vídeo, som, música, texto, e "applets" incorporadas no BitDefender), os materiais impressos que o acompanham, e quaisquer cópias do BitDefender são propriedade da SOFTWIN. O BitDefender está protegido pelos direitos de autor e pelos tratados internacionais. Assim sendo, tem de tratar o BitDefender como qualquer outro material com direitos de autor. Não pode copiar os materiais impressos que acompanham o BitDefender. Tem de produzir e incluir todos os avisos de direitos de autor na sua forma original em todas as cópias criadas independentemente dos meios ou formas, nos quais o BitDefender existe. Não pode sub-licenciar, alugar, vender, fazer leasing ou partilhar a licença BitDefender. Não pode inverter a engenharia, recompilar, desmontar, criar trabalhos derivados, modificar, traduzir, ou fazer qualquer tentativa para descobrir a fonte do código do BitDefender.

GARANTIA LIMITADA. A SOFTWIN garante que os meios, nos quais o BitDefender é distribuído, são livres de defeitos por um período de trinta dias desde a data de entrega do BitDefender a si. A única solução para uma quebra desta garantia será que a SOFTWIN, em sua opção, poderá substituir o meio defeituoso após o recebimento do produto danificado, ou reembolsar-lhe o dinheiro que pagou pelo BitDefender. A SOFTWIN não garante que o BitDefender não seja interrompido ou livre de erros, ou que os erros sejam corrigidos. A SOFTWIN não garante que BitDefender vá de encontro às suas expectativas.

EXCEPTO TAL COMO EXPRESSAMENTE EXPOSTO NESTE ACORDO, SOFTWIN RENUNCIA TODAS AS OUTRAS GARANTIAS, TANTO EXPRESSAS COMO IMPLÍCITAS, COM RESPEITO AOS PRODUTOS, MELHORIAS, MANUTENÇÃO OU SUPORTE RELACIONADOS COM ESTE ACORDO, OU QUAISQUER OUTROS MATERIAIS (TANGÍVEIS OU INTANGÍVEIS) OU SERVIÇOS FORNECIDOS POR

ELE. A SOFTWIN EXPRESSA AQUI A SUA RENÚNCIA A TODAS AS OUTRAS GARANTIAS, TANTO ESPRESSAS COMO IMPLÍCITAS, INCLUÍNDO AS GARANTIAS IMPLÍCITAS DE MERCADO, FEITAS PARA UM PROPÓSITO EM PARTICULAR, OU NÃO INTERFERÊNCIA, EXACTIDÃO DOS DADOS, EXACTIDÃO DO CONTEÚDO INFORMATIVO, INTEGRAÇÃO DE SISTEMAS, NÃO VIOLAÇÃO DE DIREITOS DE TERCEIROS AO FILTRAR, DESACTIVAR OU REMOVER O SOFTWARE DE TERCEIROS, SPYWARE, ADWARE, COOKIES, E-MAILS, DOCUMENTOS, PUBLICIDADE OU SEMELHANTE, QUER SURJAM POR ESTATUTO, LEI, NO CURSO DE TRANSAÇÕES, POR COSTUME E HÁBITO, OU USO COMERCIAL.

RENÚNCIA DE DANOS. Qualquer pessoa que use, teste, ou avalie o BitDefender suporta todo o risco pela qualidade e desempenho do BitDefender. A SOFTWIN não será responsável, em nenhuma circunstância, de qualquer dano de qualquer tipo, incluindo, sem limitação, danos directos ou indirectos provenientes do uso, desempenho, ou entrega do BitDefender, mesmo que a SOFTWIN tenha sido avisada da existência ou possibilidade de tais danos. ALGUNS ESTADOS NÃO PERMITEM A LIMITAÇÃO OU EXCLUSÃO DE RESPONSABILIDADE DE INCIDENTES OU DANOS CONSEQUENTES, POR ISSO A LIMITAÇÃO ACIMA INDICADA PODERÁ NÃO SE APLICAR A SI. EM NENHUM CASO O RISCO DA SOFTWIN PODERÁ EXCEDER O PREÇO QUE PAGOU PELO BITDEFENDER. As renúncias e limitações, estabelecidas acima, aplicar-se-ão independentemente se aceita usar, avaliar ou testar o BitDefender.

AVISO IMPORTANTE AOS UTILIZADORES. ESTE SOFTWARE NÃO É À PROVA DE FALHAS E NÃO ESTÁ DESENHADO PARA USO INTENCIONAL EM AMBIENTES DE RISCO QUE REQUEREM UMA PERFORMANCE À PROVA DE FALHAS. ESTE SOFTWARE NÃO ESTÁ INDICADO PARA SER USADO EM OPERAÇÕES DE NAVEGAÇÃO AÉREA, EM INSTALAÇÕES NUCLEARES, OU SISTEMAS DE COMUNICAÇÕES, SISTEMAS DE ARMAMENTO, DIRECTA OU INDIRECTAMENTE EM SISTEMAS DE APOIO À VIDA, CONTROLO DE TRÁFEGO AÉREO, OU QUALQUER APLICAÇÃO OU INSTALAÇÃO, ONDE A FALHA PODE RESULTAR EM MORTE, DANOS FISÍCOS GRAVES OU DANOS DE PROPRIEDADE.

GERAL. Este acordo será regido pelas leis da Roménia e pela regulamentação e tratados internacionais de direitos de autor. A jurisdição e foro exclusivo em caso de qualquer disputa que surja devido aos Termos desta Licença serão os tribunais da Roménia.

Preços, custos e taxas de uso do BitDefender estão sujeitas a alteração sem qualquer aviso prévio.

Em caso de não-validade de qualquer parte deste Acordo, a não-validade não afecta a validade das restantes partes deste Acordo.

BitDefender e o Logótipo BitDefender são marcas registadas de SOFTWIN. Todas as outras marcas registadas usadas no produto ou nos materiais associados ao mesmo são propriedade dos respectivos proprietários.

A licença cessará imediatamente e sem aviso se se encontrar a violar qualquer um dos pontos destes termos e condições. Não terá direito a um reembolso por parte de SOFTWIN ou qualquer um dos revendedores de BitDefender como resultado da cessação da licença. Os termos e condições respeitantes à confidencialidade e restrições em uso manter-se-ão em vigor mesmo após a cessação da licença.

A SOFTWIN poderá rever estes Termos a qualquer altura e os termos revistos serão automaticamente aplicáveis às versões correspondentes do Software distribuído com os termos revistos. Se qualquer parte destes Termos for encontrada como sendo desnecessária ou inaplicável, essa parte não afectará a validade dos restantes Termos, que permanecerão válidos e aplicáveis.

Em caso de controvérsia ou inconsistência entre as traduções destes Termos e outras línguas, a versão em Inglês emitida pela SOFTWIN prevalecerá sobre todas as outras.

Contacte SOFTWIN, em 5, Fabrica de Glucoza street, 72322-Sector 2, Bucharest, Romania, ou pelo Tel No: 0040-21-2330780 ou Fax:0040-21-2330763, e-mail address: <office@bitdefender.com>.

Prefácio

Este manual é dirigido a todos os utilizadores que escolheram **BitDefender Antivirus Plus v10** como a solução de segurança para os seus computadores pessoais. A informação apresentada neste manual não só é útil e acessível para as pessoas que percebam de computadores, como também é útil e acessível para todas as pessoas que sejam capazes de trabalhar com o sistema operativo Windows.

Este manual dá-lhe uma descrição completa do **BitDefender Antivirus Plus v10**, da Empresa e da equipa que o desenvolveu, também irá guiá-lo através do processo de instalação, e explicar-lhe como o pode configurar. Irá ficar a saber como usar o **BitDefender Antivírus Plus v10**, como o actualizar, testar e personalizar. Em resumo, irá ficar a saber como tirar partido do melhor que o BitDefender tem para lhe oferecer.

Desejamos-lhe uma leitura proveitosa e agradável.

1. Convenções Usadas neste Manual

1.1. Convenções Tipográficas

Diversos estilos de texto são usados neste manual para uma maior facilidade de leitura. O seu aspecto e significado são apresentados na tabela abaixo.

Aparência	Descrição
`sample syntax`	Exemplos de sintaxe são impressos em caracteres `monospace`.
http://www.bitdefender.com	O link URL está a apontar para algum local externo, num servidor http ou ftp.
`<support@bitdefender.com>`	Endereços de e-mail são inseridos no texto para contactar a solicitar mais informação.
“Prefácio” (p. xiii)	Este é um link interno, que aponta para uma área dentro do documento.
`filename`	Os ficheiros e as directorias são impressos usando a fonte `monospace`.
option	Todas as opções de produto são impressas usando caracteres a**cheio**.

Aparência	Descrição
`sample code listing`	A listagem de código é impressa com caracteres `monospace`.

1.2. Avisos

Os avisos encontram-se em notas de texto, marcadas graficamente, que lhe dão informação adicional respeitante ao parágrafo em questão.

Nota

A nota é apenas uma observação curta. Apesar de a poder omitir, a nota providencia-lhe informação valiosa, tal como uma característica específica ou um link para um determinado tópico.

Importante

Este ponto requer a sua atenção e não é recomendável ignorá-lo. Normalmente, dá-lhe informação bastante importante.

Atenção

Trata-se de informação crítica que deve de tratar com cuidados redobrados. Nada de mal acontecerá se seguir as indicações. Deve lê-la e compreendê-la, porque descreve algo extremamente arriscado.

2. A estrutura do Manual

O manual é composto de sete partes, que contêm os tópicos principais: Acerca do BitDefender, Instalação do Produto, Descrição e Características, Consola de Administração, Dicas de Utilização, CD de Emergência BitDefender e Obter Ajuda. Mais ainda, um glossário é fornecido para ajudá-lo a clarificar alguns termos técnicos.

Acerca do BitDefender. Uma breve introdução ao BitDefender.

Instalação do Produto. Instruções passo a passo para a instalação do BitDefender numa estação de trabalho. Este é um manual bastante completo de instruções sobre como instalar e usar **BitDefender Antivirus Plus v10**. Começando pelos pré-requisitos necessários para uma instalação bem-sucedida, é guiado através de todo o processo de instalação. No final, o procedimento de desinstalação é-lhe descrito para o caso de necessitar de desinstalar o BitDefender.

Descrição e Características. BitDefender Antivirus Plus v10 , as características e os módulos do produto são-lhe apresentados.

Consola de Administração. Descrição da admnistração básica e manutenção do BitDefender. Os capítulos explicam-lhe em detalhe todas as opções do **BitDefender Antivirus Plus v10**, como registar o produto, como analisar o computador e como fazer as actualizações. É-lhe ensinado como configurar e usar todos os módulos BitDefender.

Dicas de Utilização. Siga estas instruções de forma a tirar o máximo partido do seu BitDefender.

CD de Emergência BitDefender. Descrição do CD de Emergência BitDefender. Ajuda-o a compreender e a usar as características existentes neste CD de arranque.

Obter Ajuda. Onde procurar e onde pedir ajuda se algo inesperado acontecer.

Glossário. O Glossário tenta explicar alguns termos técnicos ou pouco comuns que irá encontrar nas páginas deste documento.

3. Pedido de Comentários

Convidamo-lo a ajudar-nos a melhorar este manual. Nós verificámos e testámos toda a informação com o máximo dos cuidados. Por favor escreva-nos acerca de quaisquer falhas que descubra neste manual ou a forma como acha que o mesmo poderia ser melhorado, de forma a ajudar-nos a dar-lhe a melhor documentação possível.

Faça-nos saber enviando um e-mail para <documentation@bitdefender.com>.

Importante

Por favor escreva toda a sua documentação e e-mails em inglês de forma a que possamos dar-lhes seguimento de forma eficiente.

Acerca do BitDefender

Capítulo 1. Quem é BitDefender?

BitDefender é um fabricante mundial líder em soluções de segurança que satisfazem os standards de protecção requiridos pelos ambientes informáticos. A empresa BitDefender oferece uma das linhas de software de segurança mais eficazes e modernas do mercado, que estabelecem novos padrões de prevenção de ameaças, detecção atempada e mitigação. BitDefender fornece produtos e serviços a mais de 41 milhões de utilizadores particulares e empresariais em mais de 180 paises. BitDefender possui delegações nos **Estados Unidos**, no **Reino Unido**, **Alemanha**, **Espanha** e **Roménia**.

- Contém antivírus, firewall, antispyware, antispam e controlo parental para utilizadores particulares e empresariais;
- O leque de produtos BitDefender destina-se a ser implementado em estruturas informáticas complexas (postos de trabalho, servidores de ficheiros, servidores de correio, e gateways), em plataformas Windows, Linux e FreeBSD;
- Distribuição a nível mundial, produtos disponíveis em 18 idiomas;
- Fácil de usar, com um assistente de instalação que orienta os utilizadores através do processo de instalação fazendo apenas umas poucas perguntas;
- Produtos internacionalmente certificados: Virus Bulletin, ICSA Labs, Checkmark, IST Prize, etc;
- Suporte ao cliente contínuo - a equipa de apoio ao cliente está disponível 24 horas por dia, nos 7 dias da semana;
- Tempo de resposta extremamente rápido em caso de novos ataques a computadores;
- Melhor nível de detecção;
- Actualizações de hora a hora das assinaturas de vírus via Internet - acções automáticas ou agendadas que oferecem protecção contra novos vírus.

1.1. Porquê BitDefender?

Garantido: o produtor de antivírus com maior rapidez de resposta. A rapidez de resposta de BitDefender em caso de uma epidemia de vírus ficou confirmada com os últimos surtos de vírus tais como: CodeRed, Nimda, Sircam, Badtrans.B e outros códigos maliciosos bastante perigosos, e de propagação rápida. BitDefender foi o primeiro a fornecer soluções contra estes códigos e a torná-las disponíveis de forma

gratuíta na Internet para todos aqueles que foram afectados. Agora, com a continua expansão do virus Klez – em várias versões, uma protecção antivírus tornou-se uma necessidade vital para qualquer sistema de computadores.

Inovador. Prémio de inovação pela Comissão Europeia e pela EuroCase. BitDefender foi proclamado um vencedor do European IST-Prize, atribuído pela Comissão Europeia e por representantes de 18 Academias da Europa. Agora no seu oitavo aniversário, O European IST Prize é um prémio atribuido a produtos inovadores que representam o melhor que a Europa tem em termos de inovação e informação tecnológica.

Abrangente. Protege cada ponto da sua rede, dando-lhe assim uma segurança completa. As soluções de segurança BitDefender para os ambientes empresariais satisfazem os requisitos de protecção dos diversos ambientes empresariais dos nossos dias, permitindo uma administração de todas as complexas ameaças que colocam uma rede em perigo, desde uma pequena rede local até WAN´s multi-servidor e multi-plataforma.

A Derradeira Protecção. A última fronteira para qualquer ameaça possível ao seu sistema. Como a detecção de vírus baseada na análise de código nem sempre ofereceu bons resultados, BitDefender desenvolveu uma protecção baseada em comportamento, fornecendo segurança contra malware recém-nascido.

Estes são **os custos** que as organizações querem evitar e para os quais as soluções de segurança são desenhadas para prevenir:

- Ataques de Worms
- Perdas de comunicação devido a e-mails infectados
- Quebra de recebimento de E-mails
- Limpeza e recuperação de sistemas
- Perda de produtividade experimentada pelos utilizadores de um sistema que fica indisponível
- Hacking, e acessos não autorizados que causam danos

Alguns **desenvolvimentos e benefícios** simultâneos podem ser alcançados usando a suite de segurança BitDefender:

- Aumento da disponibilidade da rede ao impedir a propagação dos ataques de código malicioso (exemplo: Nimda, Trojans (Cavalos de Tróia), DDoS).
- Protege utilizadores remotos dos ataques.
- Reduz custos administrativos de distribuição ao fazê-lo rapidamente usando as capacidades de Administração do BitDefender (soluções Empresariais).

- Impede a propagação de malware através de e-mail, usando a protecção de e-mail BitDefender na gateway da empresa. Bloqueia temporariamente ou permanentemente tentativas de ligação vulneráveis e dispendiosas de aplicações.

Mais informação acerca de BitDefender pode ser obtida visitando: http://www.bitdefender.com.

Instalação do Produto

Capítulo 2. Instalação de BitDefender Antivirus Plus v10

A secção de **Instalação de BitDefender Antivirus Plus v10** deste manual do utilizador contém os seguintes tópicos:

- Requisitos do Sistema
- Passos da instalação
- Assistente Inicial de Instalação
- Actualização
- Remover, Reparar ou Modificar o BitDefender

2.1. Requisitos do Sistema

Para um funcionamento correcto do produto, antes de instalar verifique que um dos seguintes sistemas operativos estão a ser executados no seu computador e que os correspondentes requisitos do sistema estão presentes:

2.1.1. Microsoft Windows 98 SE / NT-SP6 / Me / 2000 / XP 32-bit

- Processador Pentium II 350 MHz ou superior
- Mínimo 128 MB de Memória RAM (256 MB recomendado)
- Mínimo 60 MB de espaço disponível em disco
- Internet Explorer 5.5 ou superior

2.1.2. Microsoft Windows Vista 32-bit

- Processador 800 MHz ou superior
- Mínimo 512 MB de Memória RAM (1 GB recomendado)
- Mínimo 60 MB de espaço disponível em disco

BitDefender Antivirus Plus v10 pode ser descarregado para avaliação em http://www.bitdefender.com o site empresarial da SOFTWIN dedicado à segurança informática.

2.2. Passos da Instalação

Localize o ficheiro de instalação (setup) e clique nele duas vezes com o rato. Isto lançará o assistente que o irá guiar através do processo de instalação:

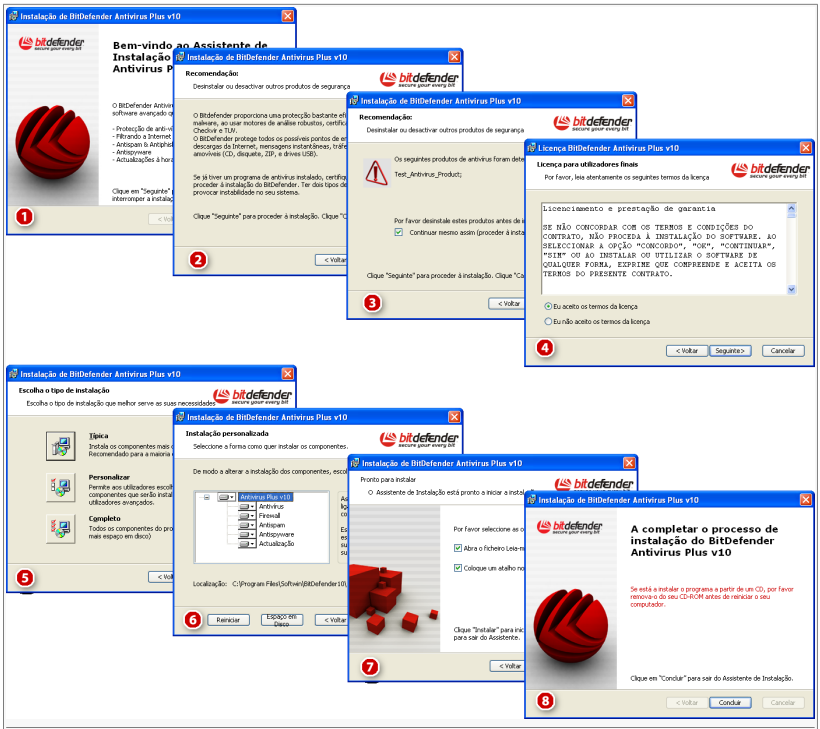
Instalação de BitDefender Antivirus Plus v10
Bem-vindo ao Assistente de Instalação do BitDefender Antivirus Plus v10
Recomendação:
Licença BitDefender Antivirus Plus v10
Licença para utilizadores finais
Licenciamento e prestação de garantia
SE NÃO CONCORDAR COM OS TERMOS E CONDIÇÕES DO CONTRATO, NÃO PROCEDA À INSTALAÇÃO DO SOFTWARE. AO SELECCIONAR A OPÇÃO "CONCORDO", "OK", "CONTINUAR", "SIM" OU AO INSTALAR OU UTILIZAR O SOFTWARE DE QUALQUER FORMA, EXPRIME QUE COMPREENDE E ACEITA OS TERMOS DO PRESENTE CONTRATO.
Eu aceito os termos da licença
Eu não aceito os termos da licença
Escolha o tipo de instalação
Típica
Personalizar
Completo
Instalação personalizada
Antivirus Plus v10
Antivirus
Firewall
Antispam
Antispyware
Actualização
Pronto para instalar
A completar o processo de instalação do BitDefender Antivirus Plus v10
Se está a instalar o programa a partir de um CD, por favor remova o do seu CD-ROM antes de reiniciar o seu computador.
Clique em "Concluir" para sair do Assistente de Instalação.
< Voltar
Seguinte >
Cancelar
Concluir
1
2
3
4
5
6
7
8

Figura 2.1. Passos da Instalação

1. Clique em **Seguinte** para continuar ou clique em **Cancelar** se pretende desistir da instalação.
2. Clique em **Seguinte** para continuar ou clique em **Retroceder** para retornar ao primeiro passo.
3. BitDefender Antivirus Plus v10 avisa-o em caso de ter outro produto antivírus instalado no seu computador.

Atenção

É altamente recomendável que desinstale qualquer outro antivírus detectado antes de instalar BitDefender. Usar dois ou mais produtos antivírus ao mesmo tempo num computador pode bloquear totalmente o seu sistema.

Clique em **Retroceder** para voltar ao passo anterior ou clique em **Cancelar** para sair da instalação. Se deseja continuar, clique em **Seguinte**.

Nota

Se BitDefender Antivirus Plus v10 não detectar outros produtos antivírus no seu sistema, pode saltar este passo.

4. Por favor leia o Acordo de Licença, seleccione **Eu aceito os termos do Acordo de Licença** e clique em **Seguinte**. Se não concordar com estes termos clique em **Cancelar**. O processo de instalação será cancelado e terminará.
5. Pode escolher o tipo de instalação que pretende: típica, personalizada ou completa.

   TÍPICA
   O programa será instalado com as opções mais comuns. Esta opção é a recomendada para a maioria dos utilizadores.

   PERSONALIZADA
   Poderá escolher os componentes que pretende instalar. Recomendada apenas para utilizadores experientes.

   COMPLETA
   Para uma instalação total do produto. Serão instalados todos os módulos do BitDefender.

   Se seleccionar **Típica** ou **Completa**, irá saltar o passo 6.
6. Se seleccionou **Personalizada**, irá aparecer uma nova janela que contém todos os componentes listados do BitDefender, para que possa seleccionar aqueles que pretende instalar.

   Se clicar em qualquer componente, irá aparecer uma breve descrição no lado direito (incluíndo o espaço mínimo requerido no disco rígido). Se clicar em qualquer ícone de um componente aparecerá uma janela onde pode escolher entre instalar ou não o módulo seleccionado.

   Pode seleccionar a pasta onde deseja instalar o produto. A pasta, por defeito, é `C:\Programas\Softwin\BitDefender 10`.

   Se deseja seleccionar outra pasta, clique em **Browse** e na janela que irá abrir, seleccione a pasta, na qual pretende que o BitDefender Antivirus Plus v10 seja instalado. Clique em **Seguinte**.

7. Tem duas opções seleccionadas, por defeito:
   - **Abrir o ficheiro Leia-me** - para abrir o ficheiro Leia-me no final da instalação.
   - **Colocar um atalho no ambiente de trabalho** - para colocar um atalho do BitDefender Antivirus Plus v10 no seu ambiente de trabalho, no final da instalação.

   Clique em **Instalar** de forma a iniciar a instalação do produto.

   Importante

   Durante o processo de instalação um assistente aparecerá. O assistente irá ajudá-lo a registar o seu**BitDefender Antivirus Plus v10**, criar uma conta BitDefender e configurar o BitDefender para executar tarefas de segurança importantes.
   Complete o processo guiado pelo assistente de forma a seguir para o próximo passo.

8. Clique em **Terminar** para completar a instalação do produto. Se aceitou as definições por defeito do caminho da instalação, irá ser criada uma pasta com o nome `Softwin` nos `Programas` que contém a subpasta `BitDefender 10`.

   Nota

   Poderá ser-lhe solicitado que reinicie o seu computador, para que o assistente de instalação possa completar o processo de instalação.

2.3. Assistente Inicial de Instalação

Durante o processo de instalação um assistente aparecerá. O assistente irá ajudá-lo a registar o seu**BitDefender Antivirus Plus v10**, criar uma conta BitDefender e configurar o BitDefender para executar tarefas de segurança importantes.

Completar a acção do assistente não é obrigatoria; no entanto, recomendamos que o faça de forma a poupar tempo e assegurar que o seu sistema fica seguro ainda antes de BitDefender Antivirus Plus v10 estar instalado.

2.3.1. Passo 1/8 - Assistente Inicial de Instalação BitDefender

Assistente de Introdução ao BitDefender
Passo 1/8
Bem-vindo ao Assistente de Introdução ao BitDefender.
Este assistente irá ajudá-lo a registar o seu produto e a activar a sua conta BitDefender. Também irá actualizar o seu BitDefender, analisar o seu sistema e ajudá-lo a agendar uma análise periódica do seu computador.
Prima 'Seguinte' para continuar o Assistente.
« Retroceder
Seguinte »
Cancelar

Figura 2.2. Janela de boas-vindas

Clique em **Seguinte**.

2.3.2. Passo 2/8 - Registar BitDefender Antivirus Plus v10.

Registo
Passo 2/8
Esta é uma versão de avaliação do BitDefender Antivirus Plus v10. Se deseja avaliar o produto, por favor escolha "Continuar a avaliar o produto". Se deseja registar o produto, escolha "Registar o produto" e insira a sua chave de licença. Poderá encontrá-la no:
- Cartão de registo do produto
- No envelope do CD-ROM
- No e-mail da sua compra On-line. Se não possui uma chave de activação por favor contacte-nos em: comercial@realsoft.pt.
Continuar a avaliar o produto
Registar o produto.
Introduzir nova chave:
Prima 'Seguinte' para continuar o Assistente.
« Retroceder
Seguinte »
Cancelar

Figura 2.3. Registo

Escolha **Registar o produto** para registar **BitDefender Antivirus Plus v10**. Insira a chave de licença no campo**Introduzir nova chave**.

Para continuar a avaliar o produto, seleccione **Continuar a avaliar o produto**.

Clique em **Seguinte**.

2.3.3. Passo 3/8 - Criar uma conta BitDefender

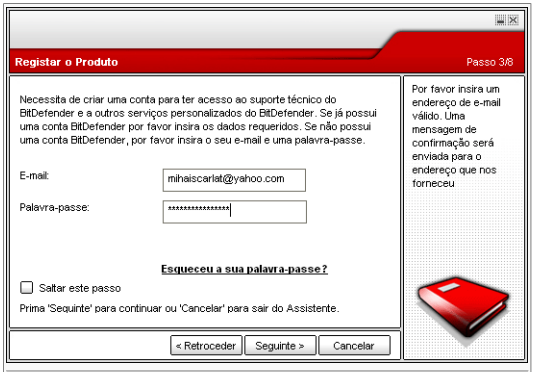
Registar o Produto
Passo 3/8
Necessita de criar uma conta para ter acesso ao suporte técnico do BitDefender e a outros serviços personalizados do BitDefender. Se já possui uma conta BitDefender por favor insira os dados requeridos. Se não possui uma conta BitDefender, por favor insira o seu e-mail e uma palavra-passe.
E-mail:
mihaiscarlat@yahoo.com
Palavra-passe:
Esqueceu a sua palavra-passe?
Saltar este passo
Prima 'Seguinte' para continuar ou 'Cancelar' para sair do Assistente.
< Retroceder
Seguinte >
Cancelar
Por favor insira um endereço de e-mail válido. Uma mensagem de confirmação será enviada para o endereço que nos forneceu

Figura 2.4. Criar uma Conta

Não tenho uma conta BitDefender

De forma a beneficiar do suporte técnico gratuíto BitDefender e outros serviços gratuítos necessita de criar uma conta.

Escreva um endereço de e-mail válido no campo**E-mail**. Crie uma palavra-passe e insira-a no campo**Palavra-passe**. Confirme a palavra-passe no campo**Re-insira palavra-passe**. Use o endereço de e-mail e a palavra-passe para ter acesso à sua conta emhttp://myaccount.bitdefender.com.

Nota

A palavra-passe deve ter pelo menos quatro caracteres em tamanho.

Para criar com sucesso uma conta deverá em primeiro lugar activar o seu endereço de e-mail. Verifique o seu endereço de e-mail e siga as instruções descrita no e-mail enviado para si pelo serviço de registo da BitDefender.

Importante

Por favor active a sua conta antes de seguir para o próximo passo.

Se não deseja criar uma conta BitDefender, seleccione **Saltar este passo**. Também irá saltar o próximo passo do assistente.

Clique em **Seguinte** para continuar ou clique em **Cancelar** para sair do assistente.

Já tenho uma conta BitDefender

Se já possui uma conta activa, use o endereço de e-mail e a palavra-passe da sua conta. Se usar uma palavra-passe incorrecta, será avisado para a inserir novamente quando clicar em **Seguinte**. Clique em **Ok** para inserir novamente a palavra-passe ou**Cancelar** para sair do assistente.

Se não se lembra da sua palavra-passe, clique em **Esqueceu a sua palavra-passe?** e siga as instruções.

Clique em **Seguinte** para continuar ou clique em **Cancelar** para sair do assistente.

2.3.4. Passo 4/8 - Inserir Detalhes da Conta

Configurar a Minha Conta
Passo 4/8
Por favor insira a informação da conta. Os dados que nos fornecer aqui serão mantidos confidenciais. Se já possui uma conta, o assistente irá mostrar-lhe a informação que nos forneceu da primeira vez que a criou.
Nome:
Scarlat
Apelido:
Mihai
País:
Romania
Prima 'Seguinte' para continuar ou 'Cancelar' para sair do Assistente.
« Retroceder
Seguinte »
Cancelar

Figura 2.5. Detalhes da Conta

Nota

Não irá passar através deste passo se seleccionou**Saltar este passo** no terceiro passo.

Insira o seu primeiro e último nome, e seleccione o país onde reside.

Se já possui uma conta, o assistente mostra-lhe a informação que nos forneceu anteriormente, se o fez. Aqui pode modificar a informação se o desejar.

Importante

Os dados que nos fornecer serão mantidos confidenciais.

Clique em **Seguinte** para continuar ou clique em **Cancelar** para sair do assistente.

2.3.5. Passo 5/8 - Aprenda acerca de RVTR

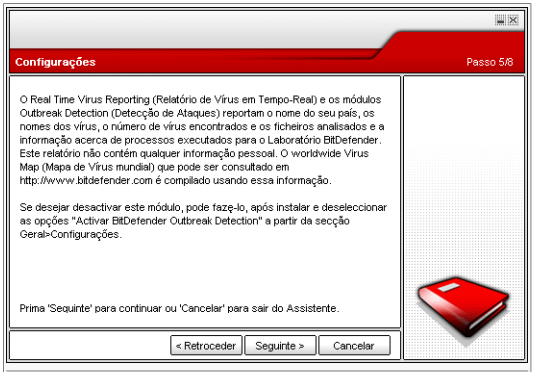
Configurações
Passo 5/8
O Real Time Virus Reporting (Relatório de Vírus em Tempo-Real) e os módulos Outbreak Detection (Detecção de Ataques) reportam o nome do seu país, os nomes dos vírus, o número de vírus encontrados e os ficheiros analisados e a informação acerca de processos executados para o Laboratório BitDefender. Este relatório não contém qualquer informação pessoal. O worldwide Virus Map (Mapa de Vírus mundial) que pode ser consultado em http://www.bitdefender.com é compilado usando essa informação.
Se desejar desactivar este módulo, pode fazê-lo, após instalar e deseleccionar as opções "Activar BitDefender Outbreak Detection" a partir da secção Geral>Configurações.
Prima 'Seguinte' para continuar ou 'Cancelar' para sair do Assistente.
« Retroceder
Seguinte »
Cancelar

Figura 2.6. Informação de RVTR

Clique em **Seguinte** para continuar ou clique em **Cancelar** para sair do assistente.

2.3.6. Passo 6/8 – Seleccionar as Tarefas a Serem Executadas

Seleccionar Tarefas
Passo 6/8
Recomendamos que actualize o seu BitDefender e leve a cabo uma análise ao sistema antes de continuar. Isto assegurará que o seu sistema está protegido desde o início.
Actualizar os motores BitDefender (poderá requer um reiniciar do pc
Executar uma análise rápida de sistema (poderá requer um reiniciar
Executar uma análise completa do sistema diária rís 2 AM.
Recomendamos que actualize o seu produto e leve a cabo uma análise ao sistema antes de continuar. Isto assegurará que o seu sistema está protegido desde o início.
Prima 'Seguinte' para continuar ou 'Cancelar' para sair do Assistente.
« Retroceder
Seguinte »
Cancelar

Figura 2.7. Selecção das Tarefas

Preparar BitDefender Antivirus Plus v10 para levar a cabo tarefas importantes para a segurança do seu sistema.

Estão disponíveis as seguintes opções:

- **Actualizar o BitDefender Antivirus Plus v10 (poderá ser necessário reiniciar)** - durante o próximo passo, será efectuada a actualização do BitDefender Antivirus Plus v10 de forma a proteger o seu computador contra as ameaças mais recentes.
- **Executar uma análise rápida (poderá ser necessário reiniciar)** -durante o próximo passo, uma análise rápida será executada de forma a que BitDefender Antivirus Plus v10 se certifique que os seus ficheiros das pastas `Windows` e `Programas` não estão infectados.
- **Executar uma análise completa diária às 2 AM** - Executa uma análise completa diária às 2 AM.

Importante

Recomendamos que tenha estas opções activas antes de avançar para o próximo passo de forma a assegurar a segurança do seu sistema.

Se seleccionar apenas a última opção ou nenhuma opção, irá saltar o próximo passo.

Pode efectuar quaisquer mudanças que queira ao retroceder para os passos anteriores (clique em **Retroceder**). Ao avançar o processo torna-se irreversível: se seleccionar continuar, deixará de ser capaz de retroceder aos passos anteriores.

Clique em **Seguinte** para continuar ou clique em **Cancelar** para sair do assistente.

2.3.7. Passo 7/8 - Esperar que as Tarefas Terminem

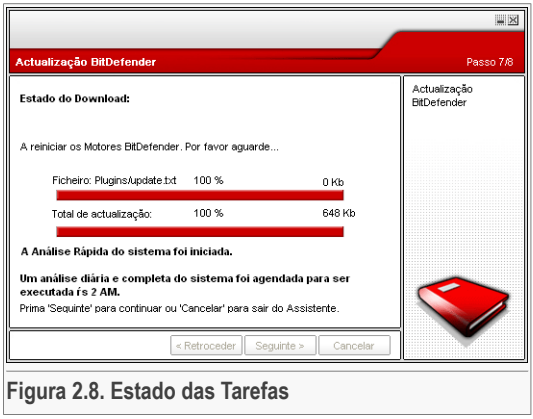
Actualização BitDefender
Passo 7/8
Estado do Download:
A reiniciar os Motores BitDefender. Por favor aguarde...
Ficheiro: Plugins/update.txt 100 % 0 Kb
Total de actualização: 100 % 648 Kb
A Análise Rápida do sistema foi iniciada.
Um análise diária e completa do sistema foi agendada para ser executada ás 2 AM.
Prima 'Seguinte' para continuar ou 'Cancelar' para sair do Assistente.
Actualização BitDefender
« Retroceder
Seguinte »
Cancelar

Figura 2.8. Estado das Tarefas

Esperar que as tarefas terminem. Pode ver o estado das tarefas seleccionadas no passo anterior.

Clique em **Seguinte** para continuar ou clique em **Cancelar** para sair do assistente.

2.3.8. Passo 8/9 - Ver Resumo

Terminar
Passo 8/8
Obrigado por avaliar o BitDefender. Por favor consulte a secção Geral»Registar para informação sobre a sua conta BitDefender e a data de expiração da sua chave de licença actual.
O BitDefender Antivirus Plus v10 foi configurado.
As seguintes tarefas foram executadas:
Os Motores BitDefender foram actualizados.
A análise rápida do sistema foi executada.
A análise completa do sistema foi agendada para ser executada todos os dias ís 2 AM.
Abrir a minha Conta BitDefender (requere uma ligação í Internet)
« Retroceder
Terminar
Cancelar

Figura 2.9. Terminar

Este é o passo final do assistente de configuração.

Seleccione**Abrir a minha conta BitDefender** - para entrar na sua conta BitDefender. Necessita para tal de estar ligado à Internet.

Clique em **Terminar** para completar a acção do assistente e continuar com o processo de instalação.

2.4. Upgrade (Mudança de versão)

O procedimento de upgrade (mudança de versão) pode ser feito de uma das seguintes formas:

- **Instalar sem remover a versão anterior – para a v8 ou superior, excepto o Internet Security**

  Faça duplo-clique no ficheiro de instalação e siga o assistente descrito na secção "*Passos da Instalação*" (p. 10).

  Importante

  Durante o processo de instalação uma mensagem de erro causada pelo `serviço Filespy`, irá aparecer. Clique em **OK** para continuar com a instalação.

- **Desinstale a sua anterior versão e instale a nova – para todas as versões BitDefender**

  Em primeiro, lugar tem de remover a anterior versão, reiniciar o computador e instalar a nova versão tal como descrito na secção "*Passos da Instalação*" (p. 10).

  Importante

  Se está a fazer um upgrade da v8 ou superior recomendamos que salve as Regras da Firewall, as Configurações BitDefender, a Lista de Amigos e a Lista de Spammers. Após terminar o processo de upgrade poderá carregá-las novamente.

2.5. Remover, Reparar ou Modificar o BitDefender

Se pretende modificar, reparar or remover o **BitDefender Antivirus Plus v10**, faça o seguinte a partir do menu Iniciar do Windows: **Iniciar → Programas → BitDefender 10 → Modificar, Reparar ou Desinstalar**.

Irá ser-lhe pedido para confirmar a sua opção ao clicar em **Seguinte**. Irá aparecer uma nova janela, na qual pode seleccionar:

- **Modificar** - para seleccionar novos componentes do programa que deseja adicionar ou para seleccionar componentes já instalados que deseja remover.

  Nota

  Para aprender a completar o processo de instalação consultar o passo seis da secção "*Passos da Instalação*" (p. 10).

- **Reparar** - para reinstalar todos os componentes já instalados no passo anterior;

  Importante

  Antes de reparar o produto recomendamos que guarde as Regras da Firewall, a Lista de Amigos e a Lista de Spammers. Pode também guardar as Configurações do BitDefender e a base de dados Bayesiana. Após terminar o processo de reparação, pode carregá-las.

- **Remover** - para remover todos os componentes instalados.

  Se escolher remover o BitDefender, não ficará mais protegido contra os vírus, spyware e hackers. Se deseja que a Firewall do Windows e o Windows Defender sejam activados após desinstalar BitDefender, seleccione a correspondente caixa de selecção no próximo passo do assistente.

  Agradeciamos-lhe imenso que tomasse um pouco do seu tempo para nos informar das razões que o levaram a desinstalar o BitDefender. Seleccione a caixa de

selecção correspondente a **Enviar Opinião** e completar o formulário on-line para nos enviar as suas sugestões.

Para continuar a instalação, seleccione uma das três opções listadas acima. Recomendamos que escolha **Remover** para uma reinstalação segura. Quando o processo de desinstalação tiver terminado, recomendamos que elimine a pasta `Softwin` dos `Programas`.

Descrição e Características

Capítulo 3. BitDefender Antivirus Plus v10

A protecção completa para o seu computador pessoal!

O **BitDefender v10** foi desenhado para pesar o menos possível aos seus utilizadores, ao mesmo tempo que garante um defesa com tecnologia de ponta contra as actuais ameaças da Internet.

O **BitDefender Antivirus Plus v10** integra módulos de antivírus, antispyware, firewall e antispam num pacote de segurança completo, feito à medida das necessidades dos utilizadores de computadores em todo o mundo.

3.1. Antivírus

O propósito do módulo antivírus é assegurar a detecção e remoção de todos os vírus conhecidos. O BitDefender Antivirus possui robustos motores de análise, certificados pelos Laboratórios ICSA, Virus Bulletin, Checkmark, Checkvir e TÜV.

Detecção Proactiva. O Analisador Heurístico Comportamental em Ambientes Virtuais (B-HAVE - Behavioral Heuristic Analyzer in Virtual Environments) emula um computador-dentro-de um-computador onde partes do software são executadas de forma a verificar comportamento potencialmente malware. Esta tecnologia proprietária do BitDefender representa um novo estrato de segurança que mantém o sistema operativo livre de vírus desconhecidos ao detectar código malicioso para o qual ainda não foram desenvolvidas soluções.

Protecção Antivírus Permanente. Os novos e melhorados motores de análise do BitDefender irão analisar e desinfectar ficheiros infectados no seu acesso, minimizando a perda de dados. Assim os ficheiros infectados poderão ser recuperados, em vez de eliminados.

Detecção e Remoção de Rootkit. Um novo módulo de BitDefender busca os rootkits (programas maliciosos desenhados para controlar os computadores vitimados, enquanto permanecem ocultos) e remove-os assim que os detecta.

Análise Web. O tráfego Web é filtrado em tempo-real ainda antes de atingir o seu browser, criando assim uma experiência web segura e agradável.

Protecção de Aplicações Peer-2-Peer e IM. Examina vírus que se propagam via mensagens instantâneas e partilha de ficheiros de aplicação de software.

Protecção Total de E-mail. BitDefender funciona ao nível do protocolo POP3, bloqueando qualquer mensagem de e-mail infectada, independentemente do cliente

de e-mail usado (Outlook™, Outlook Express™ / Windows Mail™, The Bat!™, Netscape®, etc.), sem qualquer configuração adicional.

3.2. Firewall Aplicacional

O módulo da firewall filtra o tráfego da rede e controla o acesso e as permissões das aplicações quando se conectam à Internet.

Controlo do Tráfego da Internet. Define exactamente quais as ligações de saída e de entrada a permitir/negar. Define regras com respeito a determinados protocolos, portas, aplicações e/ou endereços remotos.

Controlo de Aplicação na Internet. O BitDefender mantém uma base de dados de aplicações fiáveis, e informa os utilizadores se as aplicações que estão a solicitar acesso à rede são de confiança ou não, de forma a que possam tomar uma decisão informada. De forma alternativa o BitDefender pode dar automaticamente acesso às aplicações fiáveis.

3.3. Antispam

A nova e melhorada tecnologia antispam do BitDefender emprega inovações tecnológicas espantosas que permitem-lhe adaptar-se às novas técnicas de spam à medida que surgem, e a "aprender" as preferências do utilizador para bloquear o spam enquanto mantém uma baixa taxa de e-mails legítimos marcados como spam.

Filtragem Adaptativa. BitDefender usa técnicas de análise avançadas de "clustering e neural network" para classificar o e-mail baseado nas preferências do utilizador e padrões emergentes da colecção local de e-mails. O filtro antispam Bayesiano pode ser treinado pelo utilizador (simplesmente ao classificar algum e-mail como spam ou legítimo) e também é auto-treinado, desenvolvendo continuamente novos critérios de filtragem baseados em decisões passadas.

Anti-Phishing. O novo detector BitDefender mantém o seu computador livre de e-mails maliciosos que o tentam enganar para obter a sua informação bancária ou outra informação sensível.

Filtros de Imagem, Heurísticos, de URL, Lista Branca / Lista Negra e Caracteres. Cinco tipos filtros refinam ainda mais o seu controlo sobre os e-mails. O filtro heurístico verifica os e-mails à procura de características de spam. O filtro Lista Branca / Lista Negra rejeita e-mails provenientes de endereços de spammers conhecidos e deixa que os e-mails dos seus amigos passem, o filtro URL bloqueia e-mails contendo links maliciosos enquanto que o filtro de caracteres bloqueia e-mails escritos com caracteres “estranhos”. O filtro de imagem pode decidir se as imagens embebidas nos e-mails são ou não relativas a spam.

Compatibilidade e Integração no Outlook™. O BitDefender Antispam é compatível com todos os clientes de e-mail. A barra de tarefas antispam do BitDefender no Microsoft Outlook™ e Outlook Express™ / Windows Mail™ permite que os utilizadores treinem o filtro Bayesiano.

3.4. Antispyware

Monitoriza e previne contra os perigos de spyware em tempo-real, antes que eles possam danificar o seu sistema. Ao fazer uso de uma extensa base de dados de assinaturas de spyware, o seu computador permanecerá protegido contra o spyware.

Antispyware em Tempo-Real. BitDefender monitoriza dezenas de potenciais "hotspots" no seu sistema onde o spyware poderá actuar, e também verifica quaisquer mudanças feitas ao seu sistema e ao seu software. Ameaças de spyware conhecidas são também bloqueadas em tempo-real.

Análise e Limpeza de Spyware. BitDefender pode analisar o seu sistema, ou parte dele, à procura de ameaças de spyware. A análise utiliza uma base de dados de spyware que é constantemente actualizada.

Protecção de Privacidade. O controlo de privacidade monitoriza o tráfego HTTP (web) e SMTP (e-mail) que sai do seu computador no que diz respeito a informação pessoal – tal como número de cartão de crédito, número da Segurança Social e outros itens definidos pelo utilizador (ex.: porções de palavras-passe).

Anti-Dialer. Um anti-dialer configurável evita que aplicações perigosas possam dar origem a uma conta telefónica pesada às suas custas.

3.5. Outras Características

Instalação e Uso. Um assistente de configuração inicia-se imediatamente após a instalação, ajudando os utilizadores a seleccionar as configurações de actualização mais apropriadas, a implementar uma análise agendada e a fornecer uma forma rápida para o registo e activação do produto.

Experiência do Utilizador. BitDefender redefiniu a experiência do utilizador, pondo enfâse na facilidade de uso evitando a complexidade. Como resultado, muitos dos módulos BitDefender v10 requerem menos interacção por parte do utilizador, através de um uso conveniente da automatização e aprendizagem da máquina.

Actualizações Hora-à-Hora. O seu software BitDefender será actualizado 24 vezes por dia através da Internet, de forma directa ou através do seu servidor Proxy. O produto é capaz de se reparar a si próprio se necessário, ao descarregar os ficheiros danificados ou em falta a partir dos servidores da BitDefender.

Suporte Técnico Profissional 24 horas/7 dias. Oferecido por técnicos qualificados de suporte e por acesso a uma base de dados on-line com Respostas às Perguntas mais Frequentes.

Disco de Emergência BitDefender. BitDefender Antivirus Plus v10 vem num CD de arranque (baseado em LinuxDefender), o qual pode ser utilizado para analisar/reparar/desinfectar um sistema comprometido que não consegue arrancar.

Capítulo 4. Módulos BitDefender

BitDefender Antivirus Plus v10 contém os seguintes módulos: **Geral**, **Antivírus**, **Firewall**, **Antispam**, **Antispyware**, e **Actualização**.

4.1. Módulo Geral

O BitDefender vem totalmente configurado para a máxima segurança.

No módulo Geral pode configurar o nível de segurança e executar as tarefas de segurança importantes. Aqui pode registar o seu produto e pode definir o modo de funcionamento geral do BitDefender.

4.2. Módulo Antivírus

O BitDefender protege-o de vírus, spyware e outro malware que entram no seu sistema ao analisar os seus ficheiros, mensagens de e-mail, downloads e outros conteúdos que entrem no seu sistema.

A protecção que BitDefender oferece está dividida em duas categorias:

- Análise no acesso - Previne que novos vírus, spyware e outro malware entrem no seu sistema. Isto também é chamado protecção em tempo-real – Os ficheiros são analisados quando o utilizador lhes acede. O BitDefender irá, por exemplo, analisar um documento de texto quando o abrir, e uma mensagem de e-mail quando a receber.
- Análise a-pedido - Detecta vírus, spyware e outro malware que já se encontram no seu sistema. Esta é a análise clássica iniciada pelo utilizador – Pode escolher qual a drive, pasta ou ficheiro que o BitDefender deverá analisar, e o BitDefender analisa-o – a-pedido.

4.3. Módulo Firewall

A Firewall protege o seu computador de tentativas de ligações internas e externas não-autorizadas. É bastante semelhante a um guardião do seu portão – irá manter um olhar atento na sua ligação à Internet e rastrear a quem permitir e a quem bloquear o acesso à Internet.

A firewall é essencial se tiver uma ligação de banda larga ou ADSL.

4.4. Módulo Antispam

O Spam é um problema crescente, tanto para indíviduos como para organizações. Não é bonito, não desejaria que os seus filhos o vissem, pode fazer com que seja despedido (por desperdiçar muito tempo, ou por receber pornografia no seu mail de trabalho) e não pode impedir que as pessoas o enviem. O melhor a fazer para impedir isso, é, obviamente, parar de o receber. Infelizmente, o Spam vem em muitos formatos e feitios, e é muito abundante.

4.4.1. Esquema de funcionamento

O esquema abaixo mostra como o BitDefender funciona.

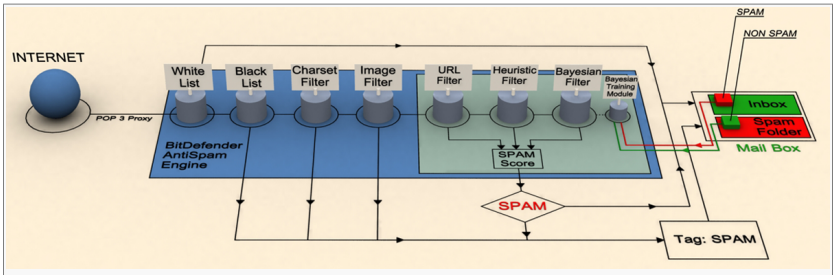

Figura 4.1. Filtros Antispam

Os filtros antispam do esquema acima (Lista Branca, Lista Negra, Filtro de caracteres, Filtro de Imagem, Filtro URL, Filtro NeuNet (Heurístico) e Filtro Bayesiano) são usados em conjunto pelo módulo Antispam do BitDefender, para determinar se uma determinada partícula de e-mail deve chegar à sua **Caixa de Entrada** ou não.

Todo o e-mail proveniente da Internet é inicialmente verificado pelo filtro da Lista Branca/Lista Negra. Se o endereço do remetente se encontrar na Lista Branca, o e-mail é movido directamente para a sua **Caixa de Entrada**.

Caso contrário, o filtro da Lista Negra irá apoderar-se do seu e-mail para verificar se o endereço do remetente se encontra na lista. O e-mail será marcado como SPAM e movido para a pasta de **Spam** (localizado no Microsoft Outlook) se houver uma correspondência.

Ainda, o Filtro caracteres irá verificar se o e-mail está escrito em caracteres Cirílicos ou Asiáticos. Se assim for, e-mail será marcado como SPAM e movido para a pasta de **Spam**.

Se o e-mail não estiver escrito em caracteres Cirílicos ou Asiáticos, irá passar pelo Filtro de Imagem. O **Filtro de Imagem** detecta todas as mensagens de e-mail que contêm imagens anexadas com conteúdo de spam.

O Filtro URL irá procurar ligações e compará-las às ligações da base de dados do BitDefender. Em caso de corresponder, irá adiconar ao e-mail uma marca de SPAM.

O Filtro NeuNet (Heurístico) irá apoderar-se do e-mail e irá executar uma série de testes aos componentes da mensagem, procurando palavras, frases, links e outras características de SPAM. E o e-mail, dependendo do resultado será ou não marcado como SPAM.

Nota

Se o e-mail estiver marcado com SEXUALLY EXPLICIT na linha do assunto, o BitDefender irá considerá-lo como SPAM.

O módulo do Filtro Bayesiano irá seguidamente analisar a mensagem, de acordo com as informações estatísticas, tendo em conta a taxa de palavras específicas que aparecem nas mensagens classificadas como SPAM, comparadas com aquelas que não são SPAM (por si ou pelo filtro heurístico). Irá ser adicionada à mensagem uma marca de Spam.

Se a pontuação total (pontuação URL + pontuação heurística + pontuação Bayesiana) excederam a pontuação de SPAM para uma mensagem (definida pelo utilizador na secção Estado como nível de tolerância), a mensagem é considerada SPAM.

Importante

Se está a utilizar outro outro cliente de e-mail que não seja o Microsoft Outlook ou Microsoft Outlook Express deve criar uma regra para mover as mensagens de e-mail maracadas como SPAM pelo BitDefender para uma pasta de quarentena que use regularmente. O BitDefender anexa o prefixo `[SPAM]` ao assunto das mensagens consideradas como tal.

4.4.2. Filtros Antispam

O Motor Antispam do BitDefender Antispam incorpora sete filtros distintos, os quais asseguram que a sua Caixa de Entrada de correio se mantenha livre de SPAM: Lista Branca, Lista Negra, Filtro caracteres, Filtro de Imagem, Filtro URL, Filtro NeuNet (Heurístico) e Filtro Bayesiano.

Nota

Pode activar/desactivar cada um destes filtro no módulo de **Antispam**, na secção das Configuração.

Lista Branca / Lista Negra

A maioria das pessoas comunica regularmente com um grupo de pessoas, ou até mesmo recebe mensagens de empresas ou organizações no mesmo domínio. Ao utilizar as **listas de amigos ou spammers**, pode facilmente decidir de quem pretende receber e-mails (amigos) independentemente do conteúdo das mensagens, ou de quem nem sequer pretende ouvir falar novamente (spammers).

Nota

A **Lista Branca / Lista Negra** também são conhecidas como **Lista de Amigos / Lista de Spammers**.

Pode gerir a **Lista de Amigos / Lista de Spammers** através da Consola de Gestão ou através da Barra de ferramentas do Antispam.

Nota

Recomendamos que adicione os nomes e endereços de e-mail dos seus amigos à **Lista de Amigos**. O BitDefender não bloqueia mensagens dos presentes nessa lista; deste modo, a adição de amigos ajuda a assegurar a passagem de mensagens legítimas.

Filtro de caracteres

A maioria das mensagens de spam estão escritas em caracteres Cirílicos ou Asiáticos. Configure este filtro se deseja rejeitar todas as mensagens de e-mail escritas nesses caracteres.

Filtro de Imagem

Uma vez que evitar o filtro heurístico se tornou um desafio e tanto, hoje em dia as pastas de entrada dos e-mails estão cada vez mais cheias de mensagens contendo apenas uma imagem com conteúdo não-solicitado. Para fazer face a este problema crescente, BitDefender introduziu o **Filtro de Imagem** que compara a assinatura do e-mail com aquelas da base de dados do BitDefender. Em caso de igualdade o e-mail será etiquetado como SPAM.

Filtro URL

A maioria das mensagens de Spam contém ligações a vários locais da web (que por sua vez contém mais publicidade e a possibilidade de comprar). O BitDefender tem uma base de dados que contém os links para este tipo de sites.

Cada ligação URL numa mensagem de e-mail será comparada com as da base de dados URL. Em caso de coincidência, será adicionada uma classificação de spam ao e-mail.

Filtro NeuNet (Heurístico)

O **Filtro NeuNet (Heurístico)** executa uma série de testes nos componentes da mensagem (por ex., não só o cabeçalho mas também todo o corpo da mensagem, seja em formato HTML ou em texto), procurando palavras, frases, links ou outras características de SPAM.

Também detecta mensagens de e-mail com o aviso de SEXUALMENTE EXPLÍCITO no assunto. Estas mensagens são consideradas SPAM.

Nota

Desde 19 de Maio de 2004, o Spam com conteúdo de caracter sexual, tem de incluir o aviso SEXUALMENTE EXPLÍCITO: no assunto ou está sujeito a multa por violação da lei.

Filtro Bayesiano

O módulo do **Filtro Bayesiano** classifica as mensagens de acordo com informações estatísticas, que indicam a frequência com que determinadas palavras aparecem nas mensagens classificadas como SPAM, quando comparadas com aquelas que não são consideradas SPAM (por si ou pelo filtro heurístico).

Isto significa, por exemplo, se uma certa palavro de quatro letras aparece com mais frequência no SPAM, é natural assumir que existe uma maior probabilidade da próxima mensagem que a inclua, seja SPAM. São levadas em conta, todas as palavras relevantes dentro de uma mensagem. Após sintetizar a informação estatística, é computada a probabilidade da mensagem ser SPAM.

Este módulo apresenta outra característica interessante: é treinável. Adapta-se rapidamente ao tipo de mensagens recebidas pelo utilizador, e armazena informação acerca de todas elas. Para funcionar com eficácia, o filtro tem de ser treinado, o que significa, apresentar-lhe amostras de Spam e de mensagens legítimas, tal como um cão de caça é treinado a caçar uma certa presa. Ás vezes o filtro também tem de ser corrigido – ajustado quando toma uma decisão errada.

Importante

Pode corrigir o módulo Bayesiano ao usar os botões **É Spam** e **Não é Spam** da Barra de tarefas Antispam.

Nota

Cada vez que executa uma actualização:

- novas assinaturas de imagens serão adicionadas ao **Filtro de Imagem**;
- novos links serão adicionados ao **Filtro de URL**;
- novas regras serão adicionadas ao **filtro NeuNet (Heurístico)**.

Isto ajuda a aumentar a eficácia do motor Antispam.

Importante

Para o proteger contra os spammers, BitDefender pode levar a cabo actualizações automáticas. Mantenha a opção **Actualização Automática** activa.

4.5. Módulo Antispyware

BitDefender monitoriza dezenas de potenciais "hotspots" no seu sistema onde o spyware poderá actuar, e também verifica quaisquer mudanças feitas ao seu sistema e ao seu software. É bastante eficaz no bloqueio de cavalos de Tróia e outras ferramentas instaladas por hackers, que tentam comprometer a sua privacidade e enviar a sua informação pessoal, tal como números de cartão de crédito, do seu computador para o do hacker.

4.6. Módulo de Actualização

Todos os dias são encontrados e identificados novos vírus. Esta é a razão, pela qual é muito importante manter o BitDefender actualizado com as últimas assinaturas de malware. Por defeito, o BitDefender procura automaticamente actualizações a cada hora.

As actualizações existem nas seguintes formas:

- **Actualizações do motor antivírus** - à medida que surgem novas ameaças, os ficheiros que contêm as assinaturas de vírus têm de ser actualizados para assegurar uma protecção permanentemente actualizada contra elas. Esta actualização também é conhecida como **Actualização das Definições de Vírus**.
- **Actualizações do motor Antispam** - novas regras serão adicionadas ao Filtro Heurístico e ao Filtro URL e novas imagens serão adicionadas ao Filtro de Imagem. Isto irá a judar a melhorar a eficácia do seu motor Antispam. Esta actualização é também conhecida como **Actualização Antispam**.
- **Actualizações para o motor de Antispyware** - novas assinaturas de spyware serão adicionadas à base de dados. Esta actualização é também conhecida como **Actualização Antispyware**.

- **Upgrades do produto** - quando é lançada uma nova versão do produto, são introduzidas novas configurações e técnicas de análise, com o objectivo de melhorar o desempenho do produto. Esta actualização também é conhecida como **Mudança de Versão**.

Além disso, do ponto de vista de intervenção do utilizador, podemos ter em conta:

- Actualização automática - o Antivírus contacta automaticamente o servidor do BitDefender, para ver se foi lançada uma nova actualização. Se assim for, o BitDefender é actualizado automaticamente. A actualização automática pode também ser feita a qualquer altura que queira, bastando para tal, que clique no botão **Actualizar agora** do módulo de Actualização.
- Actualização manual - deve descarregar e instalar manualmente as definições de vírus mais recentes.

Consola de Administração

Capítulo 5. Geral

O **BitDefender Antivirus Plus v10** foi criado com uma consola de administração centralizada, que permite a configuração das opções de protecção de todos os módulos do BitDefender. Por outras palavras, é suficiente abrir a consola de administração para que possa aceder a todos os módulos: **Antivírus**, **Firewall**, **Antispam**, **Antispyware**, e **Actualização**.

Para aceder à consola de administração, utilize o menu do Iniciar do Windows, seguindo o caminho **Iniciar → Programas → BitDefender 10 → BitDefender Antivirus Plus v10** ou mais rapidamente, duplo-clique no **ícone BitDefender** a partir da área de notificação.

BitDefender Antivírus Plus v10
Estado
Configurações
Eventos
Registo
Acerca
Geral
Antivírus
Firewall
Antispam
Antispyware
Actualização
Tarefas Rápidas
Analisar Agora
Ultima análise: nunca
Actualizar Agora
Actualizado 3/5/2007
Bloquear Tráfego
Ultima regra: Firefox
Nível de Segurança
Internet Plus
INTERNET PLUS - Protecção ampliada
Internet
Sistema local
Recomendado para sistemas directamente ligados à Internet ou a redes que não confia. Analisa e-mails, transferências IM, e todo o tráfego de rede de forma a protegê-lo dos vírus, spyware e hackers e spam (phishing incluído).
Personalize o nível de segurança premindo o botão "Nível Pessoal".
Nível Pessoal
Por Defeito
Estado do Registo
Versão de avaliação
Introduzir Nova Chave
Bem-vindo!
Esta é a janela de administração central do BitDefender.
Pode configurar o nível de Segurança do BitDefender de acordo com as suas necessidades arrastando o marcador ao longo da escala ou pode lançar as tarefas mais frequentes: "Analisar Agora", "Actualizar Agora" e "Bloquear Tráfego".
Pode registar e activar o seu BitDefender premindo o botão "Introduzir nova chave".
Mais Ajuda
bitdefender

Figura 5.1. Consola de Administração

Do lado esquerdo da consola de administração, pode ver a barra dos módulos:

- Geral - nesta secção pode definir o nível geral de segurança e executar tarefas essenciais de segurança. Aqui também pode registar o produto e ver um resumo de todas as configurações principais de BitDefender, detalhes do produto e informação de contacto.

- Antivírus - nesta secção pode configurar o módulo do **Antivírus**.
- Firewall - nesta secção pode configurar o módulo da **Firewall**.
- Antispam - nesta secção pode configurar o módulo do **Antispam**.
- Antispyware - nesta secção pode configurar o módulo do **Antispyware**.
- Actualização - nesta secção pode configurar o módulo da **Actualização**.

No lado direito da consola de administração pode ver a informação que diz respeito à secção em que se encontra. A opção **Mais Ajuda**, colocada na parte inferior direita, abre o ficheiro de**Ajuda**.

5.1. Área de Notificação

Quando a consola é minimizada aparece um ícone na área de notificação.

Se fizer duplo-clique neste ícone, a consola de administração irá abrir. Também clicando com o botão direito do rato sobre ele aparecerá um menu contextual. Permite-lhe uma administração rápida do BitDefender:

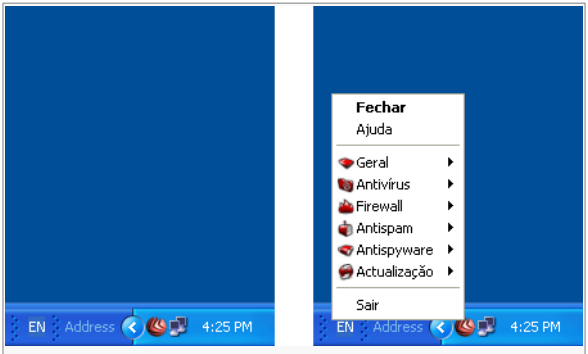

Figura 5.2. Ícone BitDefender na Área de Notificação

- **Mostrar / Fechar** - abre a consola de administração ou minimiza-a para a área de notificação.
- **Ajuda**- abre o ficheiro de ajuda.
- **Geral** - administração do módulo Geral.
  - **Introduzir Nova Chave** - inicia o assistente de registo que o guiará através do processo de registo.
  - **Editar Conta** - inicia o assistente que o ajudará a criar uma conta BitDefender.
- **Antivírus** - administração do módulo Antivírus.
  - **A protecção em Tempo-real está activada/desactivada** - mostra o estado da protecção em Tempo-real protecção em Tempo-real (activada / desactivada). Clique nesta opção para desactivar ou activar a protecção em Tempo-real.
  - **Analisar** - abre um sub-menu a partir do qual pode seleccionar executar umas das tarefas de análise disponíveis na secção Analisar.
- **Firewall** - administração do módulo da Firewall .

- A **Firewall está activada / desactivada** - mostra o estado da protecção firewall (activada / desactivada). Clique nesta opção para desactivar ou activar a protecção da firewall.
- **Bloquear todo o tráfego** - bloqueia todo o tráfego de rede / Internet.

- **Antispam** - administração do módulo Antispam.
  - **Filtro Antispam está activado / desactivado** - mostra o estado da protecção antispam (activada / desactivada). Clique nesta opção para desactivar ou activar a protecção antispam.
  - **Lista de Amigos** - abre a Lista de amigos;
  - **Lista de Spammers** - abre a Lista de Spammers.
- **Antispyware** - administração do módulo Antispyware.
  - **Antispyware Comportamental está activado / desactivado** - mostra o estado daprotecção antispyware comportamental (activada / desactivada). Clique nesta opção para desactivar ou activar a protecção antispyware comportamental.
  - **Configuração Avançada** permite-lhe configurar os comandos antispyware.
- **Actualização** - administração do módulo Actualização.
  - **Actualizar agora** - executa uma actualização imediata.
  - **Actualização automática está activada / desactivada** - mostra o estado da actualização automática (activada / desactivada). Clique nesta opção para activar ou desactivar a actualização automática.
- **Sair** - fecha a aplicação. Ao seleccionar esta opção, o ícone da área de notificação irá desaparecer e para que possa aceder à consola de administração, terá de o executar novamente através do Menu Iniciar do Windows.

Nota

O ícone ficará negro, se desactivar um ou mais dos módulos BitDefender. Desta forma saberá se alguns dos módulos estão desactivados sem ter que abrir a consola de administração.
O ícone começará a piscar sempre que esteja disponível uma actualização.

5.2. Barra de Actividade da Análise

A **Barra de Actividade da Análise** é um gráfico de visualização da actividade da análise no seu sistema.

As barras verdes (a **zona PC**) mostram o número de ficheiros analisados por segundo, numa escala de 0 a 50.

As barras vermelhas apresentadas na **zona Net** mostram o número de Kbytes transferidos (enviados e recebidos da Internet) a cada segundo, numa escala de 0 a 100.

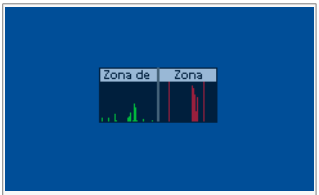

Figura 5.3. Barra de Actividade

Nota

A **barra de actividade da Análise** avisa-o quando a protecção em Tempo-real ou a Firewall está desactivada com uma cruz vermelha sobre a área correspondente (**zona PC** ou **zona Net**). Desta forma saberá se está protegido sem ter que abrir a consola de administração.

Quando quiser deixar de ver o gráfico de visualização, faça clique com o botão direito do rato sobre ele e seleccione **Esconder**.

Nota

Para fazer desaparecer esta janela definitivamente, desactive a opção **Activar a barra de Actividade da Análise** (a partir do módulo **Geral**, na secção Configuração).

Capítulo 6. Módulo Geral

A secção **Geral** deste manual do utilizador contém os seguintes tópicos:

- Administração Central
- Configuração da Consola de Administração
- Eventos
- Registo do Produto
- Acerca

Nota

Para mais detalhes com respeito ao módulo **Geral** verifique a descripção do "*Módulo Geral*" (p. 27).

6.1. Administração Central

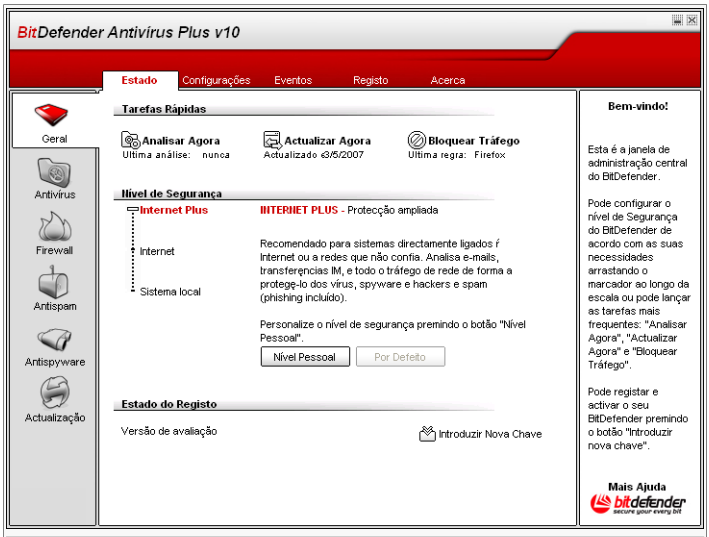
BitDefender Antivírus Plus v10
Estado
Configurações
Eventos
Registo
Acerca
Geral
Antivírus
Firewall
Antispam
Antispyware
Actualização
Tarefas Rápidas
Analisar Agora
Ultima análise: nunca
Actualizar Agora
Actualizado 03/5/2007
Bloquear Tráfego
Ultima regra: Firefox
Nível de Segurança
Internet Plus
INTERNET PLUS - Protecção ampliada
Internet
Sistema local
Recomendado para sistemas directamente ligados à Internet ou a redes que não confia. Analisa e-mails, transferências IM, e todo o tráfego de rede de forma a protegê-lo dos vírus, spyware e hackers e spam (phishing incluído).
Personalize o nível de segurança premindo o botão "Nível Pessoal".
Nível Pessoal
Por Defeito
Estado do Registo
Versão de avaliação
Introduzir Nova Chave
Bem-vindo!
Esta é a janela de administração central do BitDefender.
Pode configurar o nível de Segurança do BitDefender de acordo com as suas necessidades arrastando o marcador ao longo da escala ou pode lançar as tarefas mais frequentes: "Analisar Agora", "Actualizar Agora" e "Bloquear Tráfego".
Pode registar e activar o seu BitDefender premindo o botão "Introduzir nova chave".
Mais Ajuda
bitdefender

Figura 6.1. Administração Central

Nesta secção pode configurar o nível de segurança geral e executar tarefas importantes do BitDefender. Pode também registar o produto e ver a sua data de expiração.

6.1.1. Tarefas Rápidas

BitDefender permite-lhe um rápido acesso a tarefas essenciais de segurança. Usando essas tarefas pode manter o seu BitDefender actualizado, analisar o seu sistema ou bloquear o tráfego.

Para analisar todo o sistema basta clicar em **Analisar Agora**. A janela de análise [74] aparecerá e uma análise completa do sistema terá início.

Importante

Recomendamos-lhe vivamente que execute uma análise completa do sistema uma vez por semana. Para mais detalhes acerca das tarefas de análise e dos processos de análise consulte a secção Análise A-pedido deste manual do utilizador.

Antes de analisar o seu sistema, recomendamos que actualize o seu BitDefender de forma a que ele possa detectar as mais recentes ameaças. Para actualizar o BitDefender clique em **Actualizar Agora**. Aguarde alguns segundos até que o processo de actualização termine ou, consulte a secção Actualização para ver o seu estado de actualização.

Nota

Para mais detalhes acerca do processo de actualização consulte a secção Actualização Automática deste manual do utilizador.

Para bloquear toda a rede / Tráfego Internet clique em **Bloquear Tráfego** e depois escolha **Sim** para confirmar a sua opção. Isto irá isolar o seu computador de qualquer outro computador na rede.

Para desbloquer o tráfego mais tarde, basta clicar em **Desbloquear Tráfego**.

Nota

Para aprender a proteger de forma eficaz o seu computador numa rede de que faz parte, consulte o capítulo Módulo Firewall deste manual do utilizador.

6.1.2. Nível de Segurança

Pode escolher o nível de segurança que melhor se adapta às suas necessidades de protecção. Arraste o mostrador ao longo da escala para definir o nível de segurança apropriado.

Existem 3 níveis de segurança:

Nível de Segurança	Descrição
Sistema Local	Oferece protecção standard, especialmente recomendada para computadores sem acesso à rede ou à Internet. O consumo de recursos é baixo. Os ficheiros acedidos são analisados em busca de vírus e spyware.
Internet	Oferece protecção standard aos computadores ligados directamente à Internet ou a redes não-fiáveis. O consumo de recursos é moderado. Ficheiros acedidos, e-mails, transferências IM e todo o tráfego de rede são analisados de forma a serem protegidos dos vírus, spyware e hackers.

Nível de Segurança	Descrição
Internet Plus	Oferece protecção avançada aos computadores ligados directamente à Internet ou a redes não-fiáveis. O consumo de recursos é moderado. Ficheiros acedidos, e-mails, transferências IM e todo o tráfego de rede são analisados de forma a serem protegidos dos vírus, spyware, hackers e spam (phishing incluído).

Pode personalizar o nível de segurança clicando em **Nível personalizado**. Na janela que aparecerá, seleccione as opções de protecção do BitDefender que deseja activar e clique em **OK**.

Clique em **Nível por Defeito** para colocar o mostrador no nível por defeito.

6.1.3. Estado do Registo

Esta secção contém informação acerca do estado das licenças do seu BitDefender. Aqui, pode registar o produto e ver a sua data de expiração.

Para introduzir uma nova chave clique em **Introduzir Nova Chave**. Complete o assistente de registo para registar devidamente o BitDefender.

Nota

Para mais detalhes acerca do processo de registo consulte a secção Registo do Produto deste manual do utilizador.

6.2. Configurações da Consola de Administração

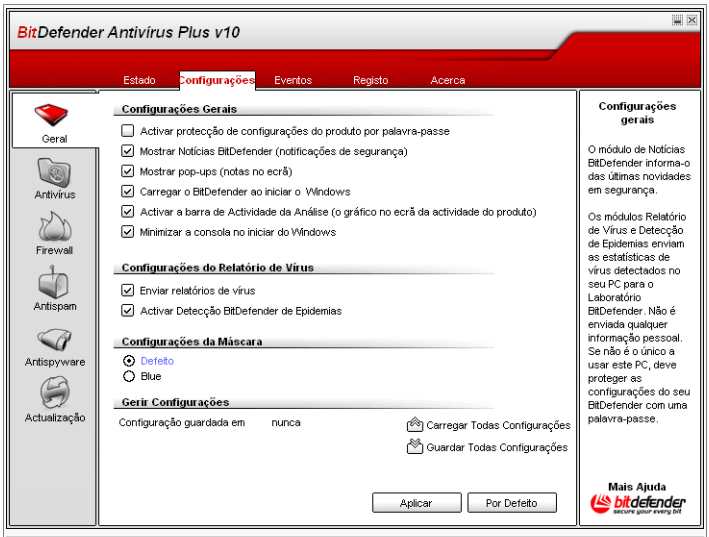
BitDefender Antivírus Plus v10
Estado
Configurações
Eventos
Registo
Acerca
Geral
Antivírus
Firewall
Antispam
Antispyware
Actualização
Configurações Gerais
Activar protecção de configurações do produto por palavra-passe
Mostrar Notícias BitDefender (notificações de segurança)
Mostrar pop-ups (notas no ecrã)
Carregar o BitDefender ao iniciar o Windows
Activar a barra de Actividade da Análise (o gráfico no ecrã da actividade do produto)
Minimizar a consola no iniciar do Windows
Configurações do Relatório de Vírus
Enviar relatórios de vírus
Activar Detecção BitDefender de Epidemias
Configurações da Máscara
Defeito
Blue
Gerir Configurações
Configuração guardada em nunca
Carregar Todas Configurações
Guardar Todas Configurações
Aplicar
Por Defeito
Configurações gerais
O módulo de Notícias BitDefender informa-o das últimas novidades em segurança.
Os módulos Relatório de Vírus e Detecção de Epidemias enviam as estatísticas de vírus detectados no seu PC para o Laboratório BitDefender. Não é enviada qualquer informação pessoal. Se não é o único a usar este PC, deve proteger as configurações do seu BitDefender com uma palavra-passe.
Mais Ajuda
bitdefender

Figura 6.2. Configurações da Consola de Administração

Aqui, pode definir o comportamento geral do BitDefender. Por defeito, o BitDefender é carregado ao iniciar o Windows e é executado minimizado na barra de tarefas.

6.2.1. Configurações Gerais

- **Activar protecção das configurações por palavra-passe** - activa a definição de uma palavra-passe de forma a proteger a configuração da Consola de Administração do BitDefender.

  Nota

  Se não for a única pessoa a utilizar este computador, recomendamos que protega as suas configurações do BitDefender com uma palavra-passe.

  Se seleccionar esta opção, a próxima janela aparecerá:

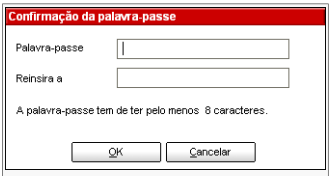

Figura 6.3. Inserir a palavra-passe

Introduza a palavra-passe no campo **Palavra-passe**, insira-a novamente no campo **Inserir de novo** e clique em **OK**.

De agora em diante, se pretender modificar as opções de configuração do BitDefender, ser-lhe-á pedido para introduzir a palavra-passe.

Importante

Se se esqueceu da palavra-passe, terá de reparar o produto para que possa modificar a configuração do BitDefender.

- **Mostrar Notícias BitDefender (notificações de segurança)** - mostra de tempos em tempos, notificações de segurança relacionadas com epidemias de vírus, enviadas pelo servidor do BitDefender.
- **Mostrar pop-ups (notas no ecrã)** - apresenta uma janela de pop-up no windows que mostra o estado do produto.
- **Carregar o BitDefender ao iniciar o Windows** - executa automaticamente o BitDefender ao iniciar o sistema.

Nota

Recomendamos que mantenha esta opção seleccionada.

- **Activar a barra de Actividade da Análise (gráfico no ecrã da actividade do produto)** - activa/desactiva a Barra de Actividade da Análise.
- **Minimizar a Consola ao Iniciar** - minimiza a consola de administração do BitDefender após ter sido carregada no iniciar do sistema. Apenas o ícone BitDefender aparecerá na Área de notificação.

6.2.2. Configurações do Relatório de Vírus

- **Enviar relatórios de vírus** - envia relatórios de vírus que foram encontrados no seu computador para os Laboratórios do BitDefender. Ajuda-nos a rastrear as epidemias de vírus.

Os relatórios não contêm dados confidenciais, tais como o seu nome, endereço de IP ou outros, e não serão usados para fins comerciais. A informação fornecida contém apenas o nome do vírus e será usada, somente para criar relatórios estatísticos.

- **Activar Detecção de Epidemias BitDefender** - envia relatórios para os Laboratórios do BitDefender com respeito a potenciais epidemias de vírus.

  Os relatórios não contêm dados confidenciais, tais como o seu nome, endereço de IP ou outros, e não serão usados para fins comerciais. A informação fornecida contém apenas o potencial vírus e será usada somente para ajudar a detectar novos vírus.

6.2.3. Configurações da Máscara

Permite-lhe seleccionar a cor da consola de administração. A máscara representa a imagem de apoio da interface. Para seleccionar uma máscara diferente, clique na cor correspondente.

6.2.4. Configurações de Administração

Use os botões **Guardar todas as Configurações** / **Carregar todas as Configurações** para guardar/carregar as configurações que tenha feito ao BitDefender para/de um determinado sítio à sua escolha. Desta forma pode usar as mesmas configurações após reinstalar ou reparar o seu produto BitDefender.

Importante

Apenas os utilizadores com direitos de administrador podem guardar ou carregar configurações.

Para carregar as configurações por defeito, clique em **Restaurar Configurações por Defeito**.

6.3. Eventos

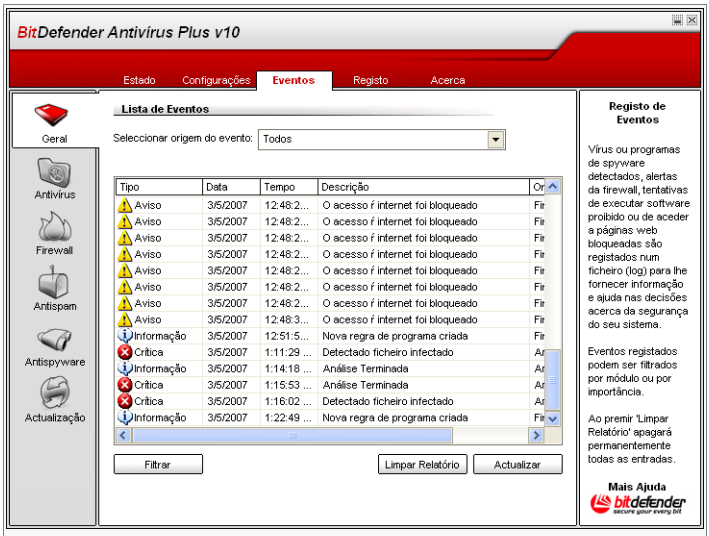
BitDefender Antivírus Plus v10
Estado
Configurações
Eventos
Registo
Acerca
Geral
Antivirus
Firewall
Antispam
Antispyware
Actualização
Lista de Eventos
Seleccionar origem do evento:
Todos
Tipo
Data
Tempo
Descrição
Aviso 3/5/2007 12:48:2... O acesso í internet foi bloqueado
Informação 3/5/2007 12:51:5... Nova regra de programa criada
Crítica 3/5/2007 1:11:29 ... Detectado ficheiro infectado
Informação 3/5/2007 1:14:18 ... Análise Terminada
Crítica 3/5/2007 1:15:53 ... Análise Terminada
Crítica 3/5/2007 1:16:02 ... Detectado ficheiro infectado
Informação 3/5/2007 1:22:49 ... Nova regra de programa criada
Filtrar
Limpar Relatório
Actualizar
Registo de Eventos
Vírus ou programas de spyware detectados, alertas da firewall, tentativas de executar software proibido ou de aceder a páginas web bloqueadas são registados num ficheiro (log) para lhe fornecer informação e ajuda nas decisões acerca da segurança do seu sistema.
Eventos registados podem ser filtrados por módulo ou por importância.
Ao premir 'Limpar Relatório' apagará permanentemente todas as entradas.
Mais Ajuda
bitdefender

Figura 6.4. Eventos

Nesta secção são mostrados todos eventos gerados pelo BitDefender.

Temos 3 tipos de eventos: **Informação**, **Aviso** e **Crítico**.

Exemplos de eventos:

- **Informação** - quando um e-mail foi analisado;
- **Aviso** - quando um ficheiro suspeito foi detectado;
- **Crítico** - quando um ficheiro infectado foi detectado.

Para cada evento a seguinte informação é disponibilizada: a data e a hora em que ocorreu, uma pequena descrição e a sua origem (**AntivírusFirewall**, **Antispyware** ou **Actualização**). Faça duplo-clique sobre um evento para ver as suas propriedades.

Pode filtrar estes eventos de 2 formas (por tipo ou por origem):

- Clique em **Filtrar** para seleccionar quais os tipos de evento a mostrar.
- Seleccione a origem do evento a partir do menu drop-down.

Se a consola de administração se encontra aberta na secção de **Eventos** e ao mesmo tempo um evento ocorre deve de clicar em **Actualizar** para ver esse evento.

Para apagar todos os eventos da lista clique em **Limpar Relatório** e depois**Sim** para confirmar a sua escolha.

6.4. Registo do produto

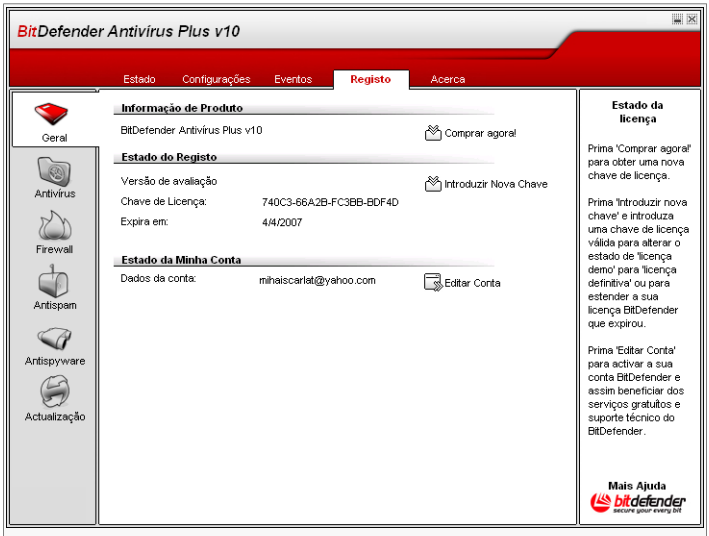

Figura 6.5. Registo do produto

Esta secção contém informação acerca do produto BitDefender (estado do registo, ID do produto, data de expiração) e da conta BitDefender. Aqui, pode registar o produto e configurar a sua conta BitDefender.

Clique no botão **Comprar Agora** para obter uma nova chave de licença da sua loja on-line local BitDefender.

Ao clicar em **Introduzir Nova Chave** pode registar o produto, modificar a chave de registo e os detalhes da sua conta. Para configurar a sua conta BitDefender clique em **Editar Conta**. Em ambos os casos, o assistente de registo aparecerá.

6.4.1. Assistente de Registo

O assistente de registo é um procedimento de 5 passos.

Passo 1/5 - Bem-vindo ao Assistente de Registo BitDefender

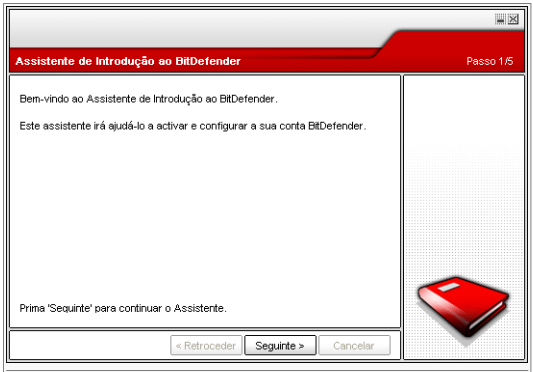
Assistente de Introdução ao BitDefender
Passo 1/5
Bem-vindo ao Assistente de Introdução ao BitDefender.
Este assistente irá ajudá-lo a activar e configurar a sua conta BitDefender.
Prima 'Seguinte' para continuar o Assistente.
« Retroceder
Seguinte »
Cancelar

Figura 6.6. Janela de boas-vindas

Clique em **Seguinte**.

Passo 2/4 - Registar BitDefender

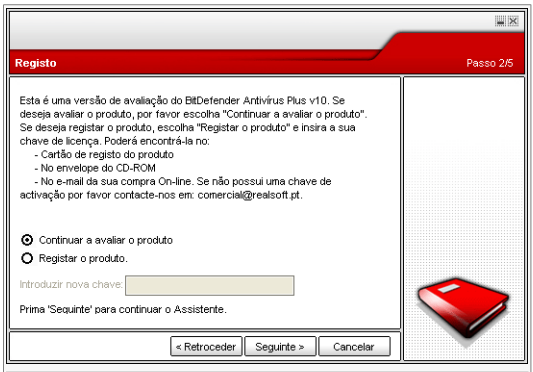
Registo
Passo 2/5
Esta é uma versão de avaliação do BitDefender Antivirus Plus v10. Se deseja avaliar o produto, por favor escolha "Continuar a avaliar o produto". Se deseja registar o produto, escolha "Registar o produto" e insira a sua chave de licença. Poderá encontrá-la no:
- Cartão de registo do produto
- No envelope do CD-ROM
- No e-mail da sua compra On-line. Se não possui uma chave de activação por favor contacte-nos em: comercial@realsoft.pt.
Continuar a avaliar o produto
Registar o produto.
Introduzir nova chave:
Prima 'Seguinte' para continuar o Assistente.
« Retroceder
Seguinte »
Cancelar

Figura 6.7. Registo

Escolha **Registar o produto** para registar **BitDefender Antivirus Plus v10**. Insira a chave de licença no campo**Introduzir nova chave**.

Para continuar a avaliar o produto, seleccione **Continuar a avaliar o produto**.

Clique em **Seguinte**.

Passo 3/5 - Criar uma Conta BitDefender

Registar o Produto
Passo 3/5
Necessita de criar uma conta para ter acesso ao suporte técnico do BitDefender e a outros serviços personalizados do BitDefender. Se já possui uma conta BitDefender por favor insira os dados requeridos. Se não possui uma conta BitDefender, por favor insira o seu e-mail e uma palavra-passe.
E-mail:
mihaiscarlat@yahoo.com
Palavra-passe:
Esqueceu a sua palavra-passe?
Saltar este passo
Prima 'Seguinte' para continuar ou 'Cancelar' para sair do Assistente.
« Retroceder
Seguinte »
Cancelar
Por favor insira um endereço de e-mail válido. Uma mensagem de confirmação será enviada para o endereço que nos forneceu

Figura 6.8. Criar uma Conta

Não tenho uma conta BitDefender

De forma a beneficiar do suporte técnico gratuíto BitDefender e outros serviços gratuítos necessita de criar uma conta.

Escreva um endereço de e-mail válido no campo**E-mail**. Crie uma palavra-passe e insira-a no campo**Palavra-passe**. Confirme a palavra-passe no campo**Re-insira palavra-passe**. Use o endereço de e-mail e a palavra-passe para ter acesso à sua conta emhttp://myaccount.bitdefender.com.

Nota

A palavra-passe deve ter pelo menos quatro caracteres em tamanho.

Para criar com sucesso uma conta deverá em primeiro lugar activar o seu endereço de e-mail. Verifique o seu endereço de e-mail e siga as instruções descrita no e-mail enviado para si pelo serviço de registo da BitDefender.

Importante

Por favor active a sua conta antes de seguir para o próximo passo.

Se não deseja criar uma conta BitDefender, seleccione **Saltar este passo**. Também irá saltar o próximo passo do assistente.

Clique em **Seguinte** para continuar.

Já tenho uma conta BitDefender

Se já possui uma conta activa, use o endereço de e-mail e a palavra-passe da sua conta. Se usar uma palavra-passe incorrecta, será avisado para a inserir novamente quando clicar em **Seguinte**. Clique em **Ok** para inserir novamente a palavra-passe ou**Cancelar** para sair do assistente.

Se não se lembra da sua palavra-passe, clique em **Esqueceu a sua palavra-passe?** e siga as instruções.

Clique em **Seguinte** para continuar.

Passo 4/5 - Inserir Detalhes da Conta

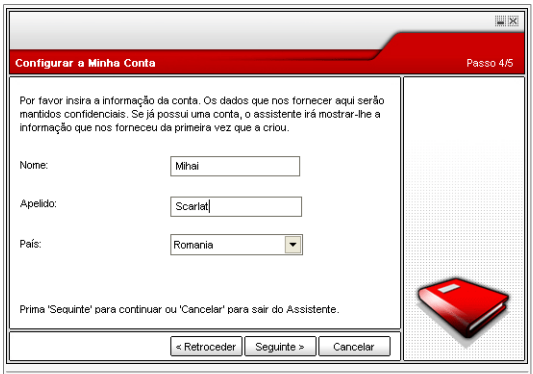
Configurar a Minha Conta
Passo 4/5
Por favor insira a informação da conta. Os dados que nos fornecer aqui serão mantidos confidenciais. Se já possui uma conta, o assistente irá mostrar-lhe a informação que nos forneceu da primeira vez que a criou.
Nome:
Mihai
Apelido:
Scarlat
País:
Romania
Prima 'Seguinte' para continuar ou 'Cancelar' para sair do Assistente.
« Retroceder
Seguinte »
Cancelar

Figura 6.9. Detalhes da Conta

Nota

Não irá passar através deste passo se seleccionou**Saltar este passo** no terceiro passo.

Insira o seu primeiro e último nome, e seleccione o país onde reside.

Se já possui uma conta, o assistente mostra-lhe a informação que nos forneceu anteriormente, se o fez. Aqui pode modificar a informação se o desejar.

Importante

Os dados que nos fornecer serão mantidos confidenciais.

Clique em **Seguinte**.

Passo 5/5 - Ver Resumo

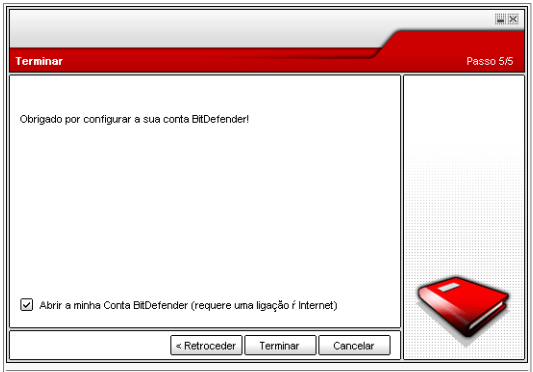

Figura 6.10. Terminar

Este é o passo final do assistente de configuração. Pode fazer as alterações que desejar, retrocedendo para os passos anteriores (clique em **Retroceder**).

Se não deseja fazer quaisquer modificações, clique em **Terminar** para sair do assistente.

Seleccione**Abrir a minha conta BitDefender** - para entrar na sua conta BitDefender. Necessita para tal de estar ligado à Internet.

6.5. Acerca

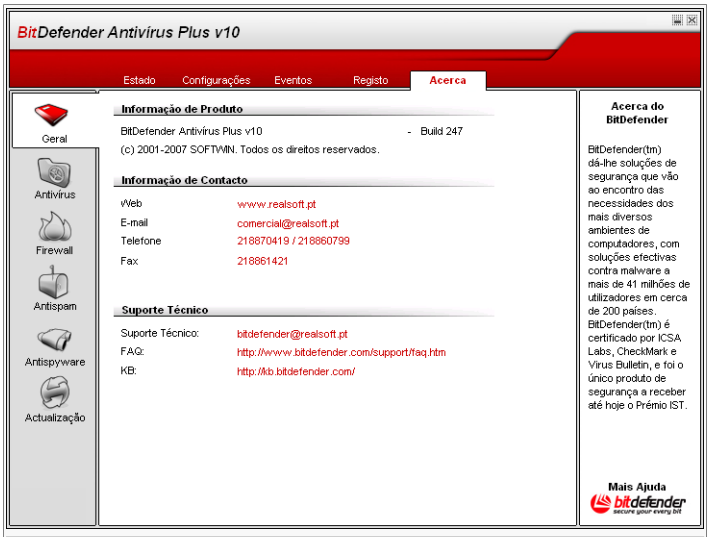

Figura 6.11. Informação Geral

Nesta secção pode encontrar a informação de contacto e os detalhes do produto.

BitDefender™ é um fabricante mundial líder em soluções de segurança que satisfazem os standards de protecção requiridos pelos ambientes informáticos. A empresa BitDefender oferece uma das linhas de software de segurança mais eficazes e modernas do mercado, que estabelecem novos padrões de prevenção de ameaças, detecção atempada e mitigação. BitDefender fornece produtos e serviços a mais de 41 milhões de utilizadores particulares e empresariais em mais de 180 paises.

O BitDefender™ é certificado pelos principais certificadores independentes - **ICSA Labs**, **CheckMark** e **Virus Bulletin**, e foi o único produto de segurança a receber um prémio **IST**.

Mais informação acerca de BitDefender pode ser obtida visitando: http://www.bitdefender.com.

Capítulo 7. Módulo Antivírus

A secção do **Antivírus** deste manual do utilizador contém os seguintes tópicos:

- Análise No-acesso
- Análise A-pedido
- Quarentena

Nota

Para mais detalhes com respeito ao módulo **Antivírus** verifique a descripção do "*Módulo Antivírus*" (p. 27).

7.1. Análise No-acesso

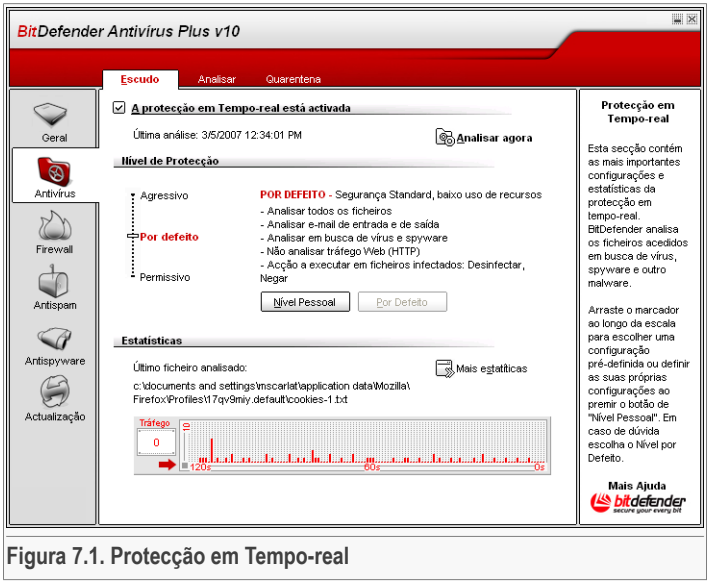
BitDefender Antivírus Plus v10
Escudo
Analisar
Quarentena
Geral
Antivírus
Firewall
Antispam
Antispyware
Actualização
A protecção em Tempo-real está activada
Última análise: 3/5/2007 12:34:01 PM
Analisar agora
Nível de Protecção
Agressivo
Por defeito
Permissivo
POR DEFEITO - Segurança Standard, baixo uso de recursos
- Analisar todos os ficheiros
- Analisar e-mail de entrada e de saída
- Analisar em busca de vírus e spyware
- Não analisar tráfego Web (HTTP)
- Acção a executar em ficheiros infectados: Desinfectar, Negar
Nível Pessoal
Por Defeito
Estatísticas
Último ficheiro analisado:
Mais estatíticas
c:\documents and settings\nscarlat\application data\Mozilla\Firefox\Profiles\17qv9miy.default\cookies-1.txt
Tráfego
0
120s
60s
0s
Protecção em Tempo-real
Esta secção contém as mais importantes configurações e estatísticas da protecção em tempo-real. BitDefender analisa os ficheiros acedidos em busca de vírus, spyware e outro malware.
Arraste o marcador ao longo da escala para escolher uma configuração pré-definida ou definir as suas próprias configurações ao premir o botão de "Nível Pessoal". Em caso de dúvida escolha o Nível por Defeito.
Mais Ajuda
bitdefender

Figura 7.1. Protecção em Tempo-real

Nesta secção pode configurar a **Protecção em Tempo-real** e pode ver informação relativa a esta actividade. A **Protecção em Tempo-real** mantém o seu computador seguro ao analisar mensagens de e-mail, downloads e os ficheiros acedidos.

Importante

Para prevenir que o seu computador seja infectado por vírus mantenha activa a **Protecção em Tempo-real**.

Na parte inferior lateral desta secção pode ver as estatísticas da análise de ficheiros e mensagens de e-mail da **Protecção em Tempo-real**. Clique em **Mais estatísticas** se desejar ver uma janela mais detalhada destas estatísticas.

7.1.1. Nível de Protecção

Pode escolher o nível de protecção que melhor se adapta às suas necessidades de segurança. Arraste o marcador ao longo da escala para definir o nível de segurança apropriado.

Existem 3 níveis de protecção:

Nível de Protecção	Descrição
Permissivo	Cobre necessidades básicas de segurança. O nível de consumo de recursos é muito baixo. Programas e mensagens de e-mail de entrada são apenas analisados em busca de vírus. Para além da tradicional análise baseada em assinaturas, a análise heurística também é utilizada. As acções levadas a cabo em ficheiros infectados são as seguintes: limpar ficheiro/negar acesso.
Por Defeito	Oferece segurança standard. O nível de consumo de recursos é baixo. Todos os ficheiros e mensagens de e-mail de entrada e saída são analisados em busca de vírus e spyware. Para além da tradicional análise baseada em assinaturas, a análise heurística também é utilizada. As acções levadas a cabo em ficheiros infectados são as seguintes: limpar ficheiro/negar acesso.
Agressivo	Oferece uma segurança elevada. O nível de consumo de recursos é moderado. Todos os ficheiros, mensagens de e-mail de entrada e saída e tráfego web são analisados em busca de vírus e spyware. Para além da tradicional análise baseada em assinaturas, a análise heurística também é utilizada. As acções levadas a cabo em ficheiros infectados são as seguintes: limpar ficheiro/negar acesso.

Para aplicar as configurações por defeito da protecção em tempo-real clique em **Nível por Defeito**.

Os utilizadores avançados poderão querer tirar partido das configurações de análise que o BitDefender oferece. O analisador pode ser configurado para evitar extensões de ficheiros, directorias ou arquivos que sabe serem inofensivos. Isto poderá reduzir o tempo de análise e melhorar a resposta do seu computador durante uma análise.

Pode personalizar **Protecção em Tempo-real** ao clicar **Nível personalizado**. A seguinte janela aparecerá:

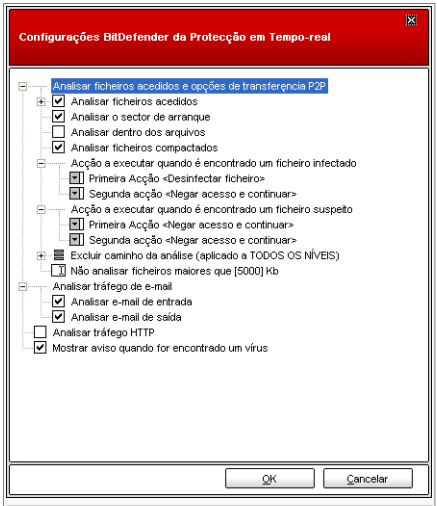

Figura 7.2. Configurações do Escudo

As opções de análise são organizadas como um menu expansível muito semelhante aos menus de exploração do Windows.

Clique na caixa com o "+" para abrir uma opção, ou na caixa com o "-" para fechar uma opção.

Pode observar que algumas opções de análise, apesar de terem o sinal "+", não podem ser abertas. Isto acontece porque estas opções ainda não foram seleccionadas. Irá observar que se as seleccionar, elas poderão ser abertas.

- **Analisar ficheiros acedidos e opções de transferências P2P** - examina os ficheiros acedidos e as comunicações feitas através de aplicações de software de Mensagens Instantâneas (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Mais adiante, seleccione o tipo de ficheiros que pretender examinar.

Opção		Descrição
Analisar ficheiros acedidos	**Analisar todos os ficheiros**	Serão analisados todos os ficheiros acedidos, independentemente do seu tipo.
	Analisar apenas os programas	Apenas os ficheiros de programas serão analisados. Isto significa, apenas os ficheiros

Opção		Descrição
		com as seguintes extensões: .exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml e .nws.
	Analisar as extensões definidas pelo utilizador	Apenas as extensões especificadas pelo utilizador serão analisadas. Estas extensões têm de estar separadas por ";".
	Excluir extensões da análise: [ ]	NÃO serão analisadas as extensões especificadas pelo utilizador. Estas extensões têm de estar separadas por ";".
	Analisar em busca de riskware	Analisa em busca de riskware. Estes ficheiros serão tratados como ficheiros infectados. O software que inclua componentes de adware poderá de deixar de funcionar se esta opção estiver activa. Seleccione **Excluir da análise dialers e aplicações** se deseja excluir este tipo de ficheiros da análise.
Analisar a unidade de disquetes no acesso		Analisa a unidade de disquetes, quando esta é acedida.
Analisar dentro dos arquivos		Os arquivos acedidos serão analisados. Com esta opção activa, o computador ficará mais lento.
Analisar ficheiros compactados		Todos os ficheiros compactados serão analisados.
Primeira Acção		Seleccionar do menu drop-down a primeira acção a levar a cabo sobre um ficheiro infectado ou suspeito.
	Negar acesso e continuar	Em caso de detecção de um ficheiro infectado, o acesso ao mesmo será negado.

Opção		Descrição
	Limpar Ficheiro	Desinfecta o ficheiro infectado.
	Apagar Ficheiro	Apaga imediatamente e sem qualquer aviso, os ficheiros infectados.
	Mover ficheiro para a quarentena	Os ficheiros infectados são movidos para a quarentena.
Segunda Acção		Seleccionar do menu drop-down a segunda acção a levar a cabo sobre um ficheiro infectado, caso a primeira acção falhe.
	Negar acesso e continuar	Em caso de detecção de um ficheiro infectado, o acesso ao mesmo será negado.
	Apagar Ficheiro	Apaga imediatamente e sem qualquer aviso, os ficheiros infectados.
	Mover ficheiro para a quarentena	Os ficheiros infectados são movidos para a quarentena.
Não analisar ficheiros maiores do que [x] Kb		Insira o tamanho máximo dos ficheiros a serem analisados. Se o tamanho for 0 Kb, todos os ficheiros serão examinados, independentemente do seu tamanho.
Excluir caminho da análise (aplica-se a TODOS OS NÍVEIS)		Clique em "+" correspondente a esta opção para especificar uma pasta que será excluída da análise. A consequência disto será que a opção irá expandir-se e aparecerá uma nova opção, um `Novo item` Clique na caixa de selecção correspondente do novo item e a partir da janela de exploração seleccione a pasta que pretende excluir da análise. Os objectos seleccionados aqui serão excluidos da análise, independentemente do nível de protecção escolhido (não apenas para o **Nível Personalizado**).

- **Analisar tráfego de e-mail** - analisa o tráfego de e-mail.

  Estão disponíveis as seguintes opções:

Opção	Descrição
Analisar e-mail de entrada	Analisa todas as mensagens de e-mail de entrada.
Analisar e-mail de saída	Analisa todas as mensagens de e-mail de saída.

- **Analisar tráfego HTTP** - Analisa o tráfego HTTP.
- **Mostrar aviso quando for encontrado um vírus** - quando um vírus é encontrado num ficheiro ou numa mensagem de e-mail, irá aparecer uma janela de alerta.

  A janela de alerta de um ficheiro infectado, contém o nome e o caminho para o vírus, a acção levada a cabo pelo BitDefender e um link para o site do BitDefender onde poderá encontrar mais informação acerca dele. No caso de um e-mail infectado, a janela de alerta contém também informação acerca do remetente e do destinatário.

  Em caso de ser detectado um ficheiro suspeito pode executar um assistente a partir da janela de alerta que o ajudará a enviar esse ficheiro para o Laboratório BitDefender para uma análise mais avançada. Pode inserir o seu endereço de e-mail para receber informação relativa a esse relatório.

Clique em **OK** para guardar as alterações e fechar a janela.

7.2. Análise A-pedido

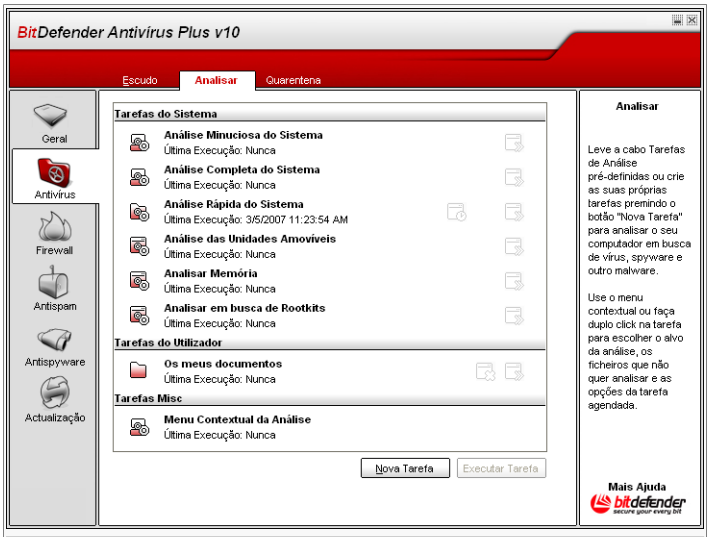
BitDefender Antivírus Plus v10
Escudo
Analisar
Quarentena
Geral
Antivírus
Firewall
Antispam
Antispyware
Actualização
Tarefas do Sistema
Análise Minuciosa do Sistema
Última Execução: Nunca
Análise Completa do Sistema
Última Execução: Nunca
Análise Rápida do Sistema
Última Execução: 3/5/2007 11:23:54 AM
Análise das Unidades Amoviveis
Última Execução: Nunca
Analisar Memória
Última Execução: Nunca
Analisar em busca de Rootkits
Última Execução: Nunca
Tarefas do Utilizador
Os meus documentos
Última Execução: Nunca
Tarefas Misc
Menu Contextual da Análise
Última Execução: Nunca
Nova Tarefa
Executar Tarefa
Analisar
Leve a cabo Tarefas de Análise pré-definidas ou crie as suas próprias tarefas premindo o botão "Nova Tarefa" para analisar o seu computador em busca de vírus, spyware e outro malware.
Use o menu contextual ou faça duplo click na tarefa para escolher o alvo da análise, os ficheiros que não quer analisar e as opções da tarefa agendada.
Mais Ajuda
bitdefender

Figura 7.3. Tarefas de Análise

Nesta secção pode configurar o BitDefender para analisar o seu computador.

O objectivo principal do BitDefender é manter o seu computador limpo de vírus. Isto é essencialmente feito ao manter os novos vírus fora do seu computador e ao analisar as suas mensagens de e-mail e quaisquer novos ficheiros descarregados ou copiados para o seu sistema.

Há o risco de um vírus já se encontrar alojado no seu sistema, mesmo antes de ter instalado o seu BitDefender. Este é o motivo pelo qual é uma excelente ideia analisar o seu computador em busca de vírus residentes depois de instalar o BitDefender. E é definitivamente uma boa ideia, analisar frequentemente o seu computador em busca de vírus.

7.2.1. Tarefas de Análise

A análise a-pedido baseia-se em tarefas de análise. O utilizador pode analisar o computador usando as tarefas por defeito ou as suas próprias tarefas de análise (tarefas definidas pelo utilizador).

Existem três categorias de tarefas de análise:

- **Tarefas do Sistema** - contém a lista das tarefas por defeito do sistema. As seguintes tarefas estão disponíveis:

Tarefa por Defeito	Descrição
Análise Minuciosa do Sistema	Analisa todo o sistema, incluindo arquivos, em busca de vírus e spyware.
Análise Completa do Sistema	Analisa todo o sistema, excepto arquivos, em busca de vírus e spyware.
Análise Rápida do Sistema	Analisa todo os programas em busca de vírus e spyware.
Analisar drives amovíveis	Analisa drives amovíveis em busca de vírus e spyware.
Analisar Memória	Analisa a memória em busca de ameaças de spyware.
Analisar em busca de Rootkits	Analisa a memória em busca de malware oculto.

- **Tarefas do Utilizador** - contém as tarefas definidas pelo utilizador.

  Uma tarefa denominada `Os meus documentos` é fornecida. Use esta tarefa para analisar os seus documentos que se encontram na pasta `Os meus documentos`.

- **Tarefas Misc** - contém uma lista de tarefas de análise variadas. Estas tarefas de análise dizem respeito a tipos de análise alternativas que não podem ser executadas a partir desta janela. Apenas pode modificar as suas configurações ou ver os relatórios de análise.

Estão disponíveis três botões à direita de cada tarefa:

- **Agendar Tarefas** - indica que a tarefa seleccionada é agendada para mais tarde. Clique neste botão para ir para a secção Agendar a partir da janela de**Propriedades** onde pode modificar esta configuração.
- **Apagar** - remove a tarefa seleccionada.

  Nota
  Não disponível para tarefas do sistema. Não pode remover uma tarefa do sistema.

- **Analisar Agora** - executa a tarefa seleccionada dando início a uma análise imediata.

7.2.2. Menú de Atalho

Um menú de atalho está disponível para cada tarefa. Clique com o botão direito do rato sobre a tarefa para a abrir.

Os seguintes comandos estão disponíveis no menu de atalho:

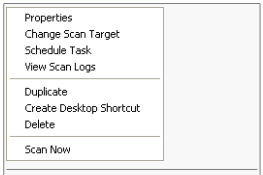

Figura 7.4. Menú de Atalho

- **Propriedades** - abre a janela das **Propriedades**, e o botão **Geral**, onde pode modificar as configurações para a tarefa seleccionada;
- **Mudar Alvo da Análise** - abre a janela das**Propriedades**e o botão **Caminho da Análise** , onde pode modificar o alvo da análise para a tarefa seleccionada;
- **Agendar Tarefa** - abre a janela das **Propriedades**e o botão **Agendar**, onde pode agendar a tarefa seleccionada;
- **Ver Relatórios de Análise** - abre a janela das**Propriedades** e a barra**Relatórios de Análise** onde pode ver os relatórios gerados após as tarefas seleccionadas terem sido executadas;
- **Duplicar** - duplica a tarefa seleccionada;

Nota

Isto é útil na criação de novas tarefas, pois pode modificar as definições da tarefa duplicada.

- **Criar Atalho no Ambiente de Trabalho** - cria um atalho no ambiente de trabalho para a tarefa seleccionada;
- **Apagar** - elimina a tarefa seleccionada;

Nota

Não disponível para tarefas do sistema. Não pode remover uma tarefa do sistema.

- **Analisar Agora** - executa a tarefa seleccionada, dando início a uma análise imediata.

Importante

Devido à sua natureza em particular, apenas as opções**Propriedades** e **Ver Relatórios de Análise** estão disponíveis para as tarefas na categoria **Tarefas Misc**.

7.2.3. Propriedades da Tarefa de Análise

Cada tarefa de análise tem as sua própria janela de**Propriedades**, onde pode configurar as opções de análise, definir o alvo da análise, agendar a tarefa ou ver os

relatórios. Para aceder a esta janela seleccione a tarefa e clique em **Propriedades** (ou clique com o botão direito do rato sobre a tarefa e depois clique em **Propriedades**).

Configurações da Análise

Aqui pode ver a informação acerca da tarefa (nome, a última vez que se executou e o seu estado de agendamento) e definir as configurações da análise.

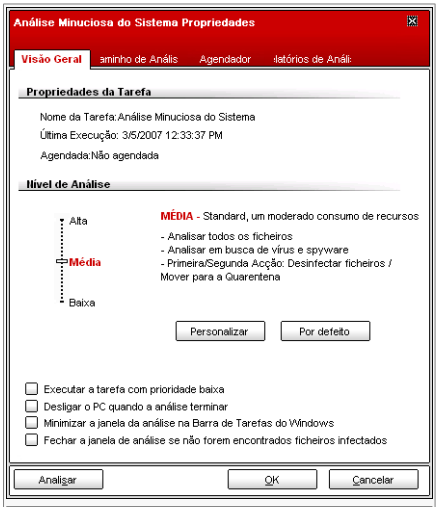
Análise Minuciosa do Sistema Propriedades
Visão Geral
aminho de Anális
Agendador
latórios de Análi
Propriedades da Tarefa
Nome da Tarefa:Análise Minuciosa do Sistema
Última Execução: 3/5/2007 12:33:37 PM
Agendada:Não agendada
Nível de Análise
Alta
Média
Baixa
MÉDIA - Standard, um moderado consumo de recursos
- Analisar todos os ficheiros
- Analisar em busca de vírus e spyware
- Primeira/Segunda Acção: Desinfectar ficheiros / Mover para a Quarentena
Personalizar
Por defeito
Executar a tarefa com prioridade baixa
Desligar o PC quando a análise terminar
Minimizar a janela da análise na Barra de Tarefas do Windows
Fechar a janela de análise se não forem encontrados ficheiros infectados
Analisar
OK
Cancelar

Figura 7.5. Configurações da Análise

Nível de Análise

Antes de mais, tem de escolher o nível de análise. Arraste o marcador ao longo da escala para definir o nível de análise apropriada.

Existem 3 níveis de análise:

Nível de Protecção	Descrição
Baixo	Oferece uma eficiência razoável de detecção. O consumo de recursos é baixo. Programas são apenas analisados em busca de vírus. Para além da tradicional análise baseada em assinaturas, a análise heurística também é utilizada. As acções levadas a cabo em ficheiros infectados são as seguintes: limpar ficheiro/mover para a quarentena.
Médio	Oferece uma boa eficiência de detecção. O nível de consumo de recursos é moderado.

Nível de Protecção	Descrição
	Todos os ficheiros são analisados em busca de vírus e spyware. Para além da tradicional análise baseada em assinaturas, a análise heurística também é utilizada. As acções levadas a cabo em ficheiros infectados são as seguintes: limpar ficheiro/mover para a quarentena.
Elevado	Oferece uma elevada eficiência de detecção. O nível de consumo de recursos é elevado. Todos os ficheiros e arquivos são analisados em busca de vírus e spyware. Para além da tradicional análise baseada em assinaturas, a análise heurística também é utilizada. As acções levadas a cabo em ficheiros infectados são as seguintes: limpar ficheiro/mover para a quarentena.

Importante

A tarefa **Analisar Rootkits** tem os mesmos níveis de análise. No entanto, as opções são diferentes:

- **Baixa** - Apenas os processos serão analisados. Não será tomada nenhuma acção nos objectos detectados.
- **Média** - Ficheiros e processos são analisados em busca de objectos ocultos. Não será tomada nenhuma acção nos objectos detectados.
- **Elevada** - Ficheiros e processos são analisados em busca de objectos ocultos. Objectos detectados são renomeados.

Os utilizadores avançados podem pretender tirar partido das configurações de análise do BitDefender. O analisador pode ser programado para evitar extensões de ficheiros, directórios ou arquivos que sabe serem inofensivos. Isto poderá reduzir os tempos de análise e melhorar a resposta do seu computador durante a mesma.

Clique em **Personalizar** - para definir as suas próprias opções de análise. Uma nova janela irá aparecer.

As opções de análise são organizadas como um menu expansível muito semelhante aos menus de exploração do Windows.

As opções de análise estão agrupadas em cinco categorias:

- **Opções de análise de vírus**
- **Opções de análise de spyware**
- **Opções de acção**
- **Opções do relatório**
- **Outras opções**

Clique na caixa com o "+" para abrir uma opção, ou na caixa com o "-" para fechar uma opção.

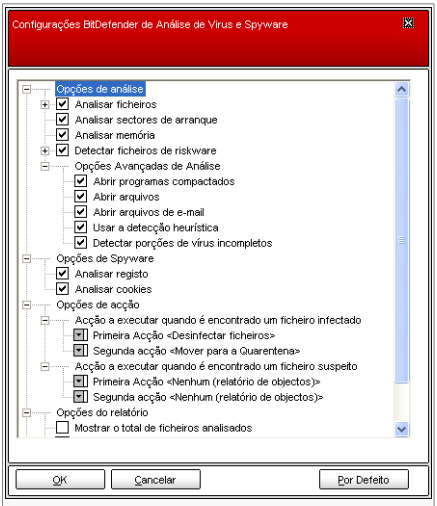

Figura 7.6. Configurações da Análise

Importante

Para a tarefa de**Análise de Rootkits** apenas três categorias estão disponíveis: **Opções de Análise de Rootkits**, **Opções de relatório** e **Outras opções**. Da primeira categoria pode escolher o que analisar (ficheiros ou memória, ou ambos) e pode definir a acção a tomar sobre os objectos detectados(**Nenhuma (Objectos do Relatório)/Renomear ficheiros**). As duas últimas categorias são idênticas às descritas abaixo.

- Especifique que tipo de objectos devem ser analisados (ficheiros, mensagens de e-mail e por aí fora) e outras opções. Isto é feito através de seleccionar determinadas opções da categoria **Opções de análise de vírus**.

Opção		Descrição
Análise de ficheiros	**Analisar todos os ficheiros**	Serão analisados todos os ficheiros acedidos, independentemente do seu tipo.
	Analisar apenas os programas	Analisa apenas ficheiros de programa. Isto significa apenas ficheiros com as seguintes extensões: `exe`; `bat`; `com`; `dll`; `ocx`; `scr`; `bin`; `dat`; `386`; `vxd`; `sys`; `wdm`; `cla`; `class`; `ovl`; `ole`; `exe`; `hlp`; `doc`; `dot`; `xls`; `ppt`; `wbk`; `wiz`; `pot`; `ppa`; `xla`; `xlt`; `vbs`; `vbe`; `mdb`; `rtf`; `htm`; `hta`; `html`; `xml`; `xtp`; `php`; `asp`; `js`; `shs`; `chm`; `lnk`;

Opção		Descrição
		pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml e nws.
	Analisar as extensões definidas pelo utilizador	Apenas as extensões especificadas pelo utilizador serão analisadas. Estas extensões têm de estar separadas por ";".
	Excluir extensões definidas pelo utilizador	NÃO serão analisadas as extensões especificadas pelo utilizador. Estas extensões têm de estar separadas por ";".
Analisar os sectores de arranque		Analisa o sector de arranque do sistema.
Analisar Memória		Analisa a memória em busca de vírus e outro malware.
Detectar ficheiros de riskware		Analisa à procura de outras ameaças para além de vírus, tais como: dialers e adware. Estes ficheiros serão tratados como ficheiros infectados. O software que inclua componentes de adware poderá de deixar de funcionar se esta opção estiver activa. Seleccione **Excepto aplicações e dialers** se pretende excluir este tipo de ficheiros da análise.
Opções avançadas de análise	**Abrir programas compactados**	Verifica todos os ficheiros compactados.
	Abrir arquivos	Analisa interior dos arquivos.
	Abrir arquivos do e-mail	Analisa o interior dos arquivos de e-mail.
	Usar a detecção heurística	Para utilizar a análise heurística dos ficheiros. O objectivo da análise heurística é identificar novos vírus, baseado em certos padrões e algoritmos, antes de haver uma nova solução para o vírus. Poderão aparecer falsas mensagens de alarme. Quando é detectado tal programa, este é classificado como suspeito. Nestes casos, recomendamos que envie o ficheiro para análise no laboratório BitDefender.

Opção	Descrição
Detectar corpos de vírus incompletos	Detecta corpos de vírus incompletos.

- Especifica os alvos de análise de spyware (registo, cookies). Isto é feito através de seleccionar determinadas opções da categoria **Opções de análise de spyware**.

Opção	Descrição
Analisar registo	Analisa entradas de registo.
Analisar cookies	Analisa os ficheiros cookie.

- Especifique a acção sobre ficheiros infectados ou suspeitos. Abra a categoria **Opções de acção** de forma a ver todas as possíveis acções sobre esses ficheiros.

  Seleccione as acções a tomar quando um ficheiro suspeito ou infectado é descoberto. Pode especificar diferentes acções para ficheiros infectados e ficheiros suspeitos. Também pode seleccionar uma segunda acção a tomar caso a primeira falhe.

Acção	Descrição
Nenhum (objectos de relatório)	Nenhuma acção será levada a cabo sobre os ficheiros infectados. Estes ficheiros aparecerão no ficheiro de relatório.
Avisar o utilizador da acção	Sempre que for eliminado um ficheiro infectado,é mostrada uma caixa de diálogo, onde o utilizador pode seleccionar a acção a desenvolver naquele ficheiro. Dependendo da importância do ficheiro, pode seleccionar a sua desinfecção, o seu isolamento na zona da quarentena ou a sua eliminação.
Desinfectar ficheiros	Desinfecta o ficheiro infectado.
Apagar ficheiros	Apaga imediatamente e sem qualquer aviso, os ficheiros infectados.
Mover ficheiros para a quarentena	Para mover os ficheiros infectados da quarentena para o seu local inicial.
Renomear ficheiros	Para modificar a extensão dos ficheiros infectados. A nova extensão dos ficheiros infectados será `.vir`. Ao renomear os ficheiros infectados, é removida a

Acção	Descrição
	possibilidade de execução e propagação da infecção. Ao mesmo tempo eles podem ser guardados para futuro exame ou análise.

Importante

Renomear ficheiros tem um efeito similar nos ficheiros ocultos (rootkits). A nova extensão dos ficheiros detectados será `.bd.ren`. Ao renomear os ficheiros infectados, é removida a possibilidade de execução e propagação da infecção. Ao mesmo tempo eles podem ser guardados para futuro exame ou análise.

- Especifique as opções dos ficheiros de relatório. Abra a categoria **Opções do relatório** de forma a ver todas as possíveis opções.

Opção	Descrição
Mostrar todos os ficheiros analisados	Lista todos os ficheiros examinados e o seu estado (infectado ou não) num ficheiro de relatório. Com esta opção ligada, o computador irá diminuir a sua rapidez.
Apagar relatórios com mais de [x] dias	Este é um campo editável que permite especificar durante quanto tempo um relatório deve ser mantido na secção Relatórios de Análise. Seleccione esta opção e insira um novo intervalo de tempo. O intervalo de tempo por defeito é de 180 dias.

Nota

Os ficheiros de relatórios podem ser visualizados na secção Relatórios da Análise a partir da janela **Propriedades**.

- Especifique as outras opções. Abra a categoria **Outras Opções** a partir da qual pode seleccionar a seguinte opção:

Opção	Descrição
Enviar os ficheiros suspeitos ao Laboratório BitDefender	Será solicitado a enviar todos os ficheiros suspeitos ao laboratório BitDefender após o processo de análise ter terminado.

Se clicar em **Nível por Defeito** carregará as configurações por defeito.

Clique em **OK** para guardar as alterações e fechar a janela.

Outras Configurações

Uma série de opções gerais estarão disponíveis para o processo de análise:

Opção	Descrição
Execute a tarefa de análise com prioridade baixa	Diminui a prioridade do processo de análise. Irá permitir que outros programas funcionem com maior rapidez e aumenta o tempo necessário para terminar o processo da análise.
Desligar o PC quando a análise terminar	Desliga o computador após terminar o processo de análise.
Enviar os ficheiros suspeitos ao Laboratório BitDefender	Será solicitado a enviar todos os ficheiros suspeitos ao laboratório BitDefender após o processo de análise ter terminado.
Minimizar a janela da análise ao iniciar para a área de notificação	Minimiza a janela da análise no Windows para a área de notificação. Faça duplo-clique sobre o ícone BitDefender para o abrir.

Clique em **OK** para guardar as alterações e fechar a janela. Para executar a tarefa, apenas clique em **Analisar**.

Alvo da Análise

Seleccione a tarefa, clique em **Propriedades** e depois clique no botão **Analisar Caminho** para entrar nesta secção.

Aqui pode definir o alvo da análise.

A secção contém os seguintes botões:

- **Adicionar ficheiro** - abre uma janela de exploração, onde pode seleccionar o(s) ficheiro(s), que pretende examinar.
- **Adicionar pasta** - tal como em cima, mas selecciona qual (quais) a(s) pasta(s) que pretende que o BitDefender analise, em vez de qual (quais) ficheiro(s).

Nota

Pode usar o drag and drop para adicionar ficheiros/pastas à lista.

- **Apagar item** - remove o(s) ficheiro (s) / pasta(s) que foram previamente seleccionados da lista dos objectos a serem analisados.

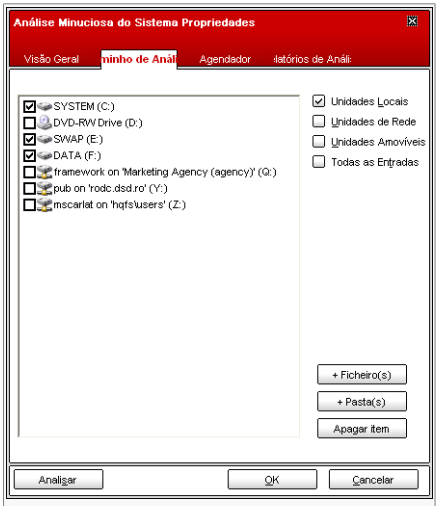

Figura 7.7. Alvo da Análise

Nota

Apenas podem ser eliminados o(s) ficheiro(s) / pasta(s) que foram adicionados posteriormente, mas não aqueles que foram automaticamente "enviados" pelo BitDefender.

Para além dos botões explicados acima existem também algumas opções que permitem uma selecção rápida das áreas a analisar.

- **Unidades Locais** - para analisar as drives locais.
- **Unidades de Rede** - para analisar todas as drives de rede.
- **Unidades Amovíveis** - para analisar todas as drives amovíveis (CD-ROM, unidade de disquetes).
- **Todas as Entradas** - para analisar todos as drives, independentemente de serem locais, de rede ou amovíveis.

Nota

Se pretende analisar em busca de vírus todo o seu computador, seleccione a caixa de selecção correspondente a **Todas as entradas**.

Clique em **OK** para guardar as alterações e fechar a janela. Para executar a tarefa, apenas clique em **Analisar**.

Agendar

Seleccione a tarefa, clique em **Propriedades** e depois clique no botão **Agendar** para entrar nesta secção.

Aqui pode ver se a tarefa está agendada ou não e aqui pode modificar essa propriedade.

Importante

Com tarefas complexas, o processo de análise leva algum tempo, e funciona melhor se fechar todos os outros programas. É por isso que é melhor agendar tais tarefas para quando não estiver a utilizar o seu computador e este tenha entrado no modo de descanso.

Figura 7.8. Agendar

Quando agendar uma tarefa, deve de escolher uma das seguintes opções:

- **Não agendada** - executa a tarefa apenas quando o utilizador a solicita.
- **Uma vez** - Executa a análise uma só vez, num determinado momento. Definir a data de início e a hora nos campos**Iniciar Data/Hora**
- **Periodicamente** - Executa a análise periodicamente, a um determinado intervalo de tempo (horas, dias, semanas, meses, anos) começando numa determinada data e hora.

  Se pretende que a análise seja repetida a um certo intervalo, seleccione a a opção **Periodicamente** e insira na caixa de edição **A cada**, o número de minutos/horas/dias/semanas/meses/anos para indicar a frequência deste processo. Deve de definir a data de início e a hora nos campos**Iniciar Data/Hora**.

Clique em **OK** para guardar as alterações e fechar a janela. Para executar a tarefa, apenas clique em **Analisar**.

Relatórios da Análise

Seleccione a tarefa, clique em **Propriedades** e depois clique no botão **Relatórios da Análise** para entrar nesta secção.

Aqui pode ver os relatórios gerados de cada vez que a tarefa foi executada. Cada ficheiro no relatório contém informação sobre o seu estado (limpo/infectado), a data e hora quando a análise foi feita e um resumo (análise terminada).

Estão disponíveis dois botões:

- **Mostrar Relatório** - para ver o relatório seleccionado.
- **Apagar Relatório** - para apagar o relatório seleccionado.

Também, para ver ou apagar um ficheiro, faça duplo-clique com o rato sobre o ficheiro e seleccione a opção correspondente do menu de atalho.

Clique em **OK** para guardar as alterações e fechar a janela. Para executar a tarefa, apenas clique em **Analisar**.

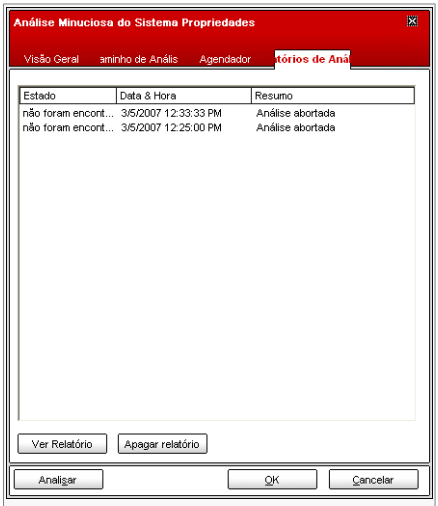

Figura 7.9. Relatórios da Análise

7.2.4. Tipos de Análise A-pedido

O BitDefender permite três tipos de análise a-pedido:

- Análise imediata - executa uma tarefa de análise das tarefas do sistema/utilizador;
- Análise contextual - faça duplo-clique com o botão direito do rato sobre um ficheiro ou pasta e seleccione BitDefender Antivirus v10;
- Análise Drag& Drop - Arraste e largue um ficheiro ou pasta em cima da Barra de Actividade da Análise;

Análise imediata

Para analisar o seu computador ou parte dele pode usar as tarefas de análise por defeito ou pode criar as suas próprias tarefas de análise. Existem dois métodos de criar tarefas de análise:

- Duplique uma tarefa de análise, renomeia-a e faça as alterações necessárias na janela Propriedades;
- Clique em **Nova Tarefa** para criar uma nova tarefa e configure-a.

Para que o BitDefender possa efectuar uma análise completa, tem de encerrar todos os programas abertos. É especialmente importante que encerre o seu programa de e-mail (por ex. Outlook, Outlook Express ou Eudora).

Antes de permitir que o BitDefender analise o seu computador, certifique-se que o BitDefender se encontra actualizado com as últimas assinaturas de vírus, dado que todos os dias são encontrados e identificados novos vírus. Pode verificar quando foi feita a última actualização, no lado superior do módulo de Actualização.

Para dar início à análise, use um dos seguintes métodos:

- faça duplo-clique com o rato sobre a tarefa desejada da lista.
- clique no botão **Analisar agora** da correspondente tarefa.
- seleccione a tarefa e depois clique em **Executar Tarefa**.

A janela da análise irá aparecer.

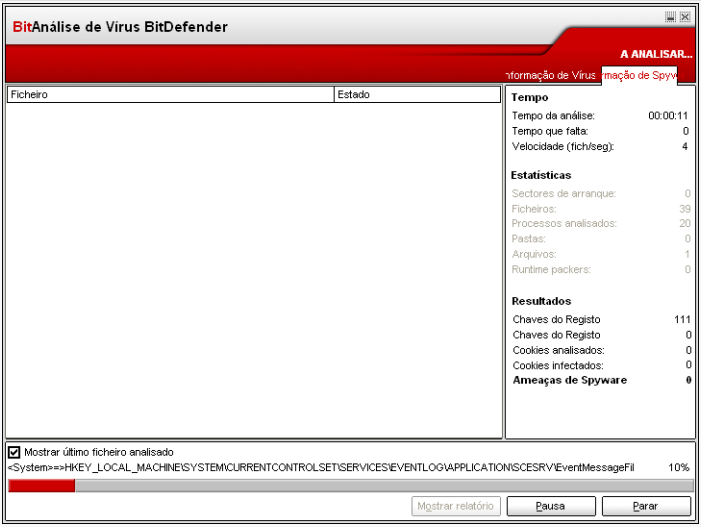

Figura 7.10. Janela da Análise

Um ícone aparecerá na área de notificação quando um processo de análise está a decorrer.

Ao fazer a análise, o BitDefender mostrará o seu progresso e alerta-o se alguma ameaça for encontrada. À direita, poderá ver as estatísticas do processo de análise. Dependendo das unidades a analisar, está disponível a informação do spyware e/ou do antivírus. Se ambas estiverem disponíveis, clique na barra correspondente para saber mais sobre processo de análise de spyware ou de vírus.

Seleccione a caixa de verificação correspondente a **Mostrar os últimos ficheiros analisados** e apenas será visível a informação acerca dos últimos ficheiros examinados.

Nota

O processo de análise pode demorar algum tempo, dependendo da complexidade da mesma.

Estão disponíveis três botões:

- **Parar** - abre uma nova janela, onde pode terminar o processo de análise. Clique em **Sim&Fechar** para sair da janela de análise.

  Nota

  Se foram detectados ficheiros suspeitos durante a análise, ser-lhe-á solicitado que os envie para o Laboratório do BitDefender.

- **Pausa** - pára temporariamente o processo de análise – pode continuá-lo ao clicar em **Retomar**.
- **Mostrar relatório** - abre o relatório da análise.

Nota

Se clicar com o botão direito do rato numa tarefa que está a ser executada, um menu de atalho (contextual) que lhe permite administrar a janela de análise aparecerá. As opções (**Pausa / Retomar**, **Parar** e **Parar&Fechar**) são similares aos botões da janela de análise.

Se a opção **Consultar utilizador sobre a acção** estiver definida na janela Propriedades, quando um ficheiro infectado é detectado uma janela de alerta irá solicitar-lhe que escolha uma acção a levar a cabo sobre o ficheiro infectado.

Pode visualizar o nome do ficheiro e do vírus.

Pode seleccionar uma das seguintes opções no ficheiro infectado:

- **Desinfectar** - para desinfectar um ficheiro infectado;
- **Eliminar** - para eliminar um ficheiro infectado;
- **Mover para a quarentena** - para mover um ficheiro infectado para a zona de quarentena;
- **Ignorar** - para ignorar a infecção. Não será tomada nenhuma acção nos ficheiros infectados.

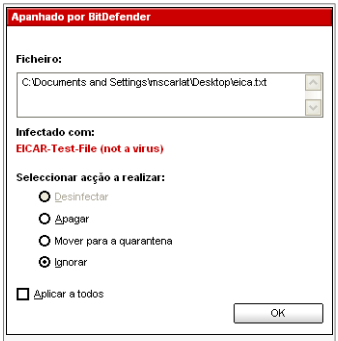

Figura 7.11. Selecção da Acção

Se analisar uma pasta, e deseja que a acção dos ficheiros infectados seja a mesma para todos, seleccione a opção **Aplicar a todos**.

Nota

Se a opção de **Desinfectar** não estiver activa, significa que o ficheiro não pode ser desinfectado. A melhor escolha será isolá-lo na zona de quarentena e enviá-lo para nós o analisarmos ou eliminá-lo.

Clique em **OK**.

Nota

O ficheiro do relatório é guardado automaticamente na secção de Relatórios da Análise a partir da janela **Propriedades** da respectiva tarefa.

Análise contextual

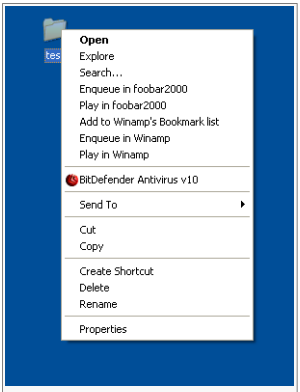

Figura 7.12. Análise contextual

Clique com o botão direito do rato sobre o ficheiro ou pasta que pretende analisar e seleccione **BitDefender Antivirus v10**.

Pode modificar as opções de análise e ver os relatórios ao aceder à janelas das Propriedades da tarefa **Análise de Menu Contextual**.

Análise por Drag&Drop

Arraste o ficheiro ou a pasta que pretende analisar e deixe-a cair em cima da **Barra de Actividade da Análise**, como apresentado abaixo.

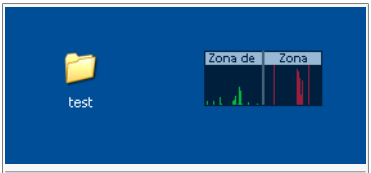

Figura 7.13. Arraste o ficheiro

Se um ficheiro infectado é detectado uma janela de alerta aparecerá a solicitar-lhe que seleccione a acção a ser levada a cabo sobre o ficheiro infectado.

Em ambas as alternativas de análise (contextual e drag&drop) irá aparecer uma janela de análise [74]

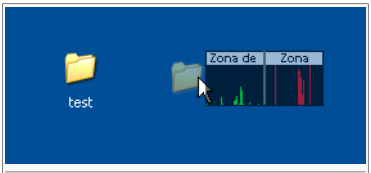

Figura 7.14. Deixe cair o ficheiro

7.2.5. Análise de Rootkits

BitDefender surge para resolver as mais recentes ameaças de segurança ao introduzir um detector de rootkits adicionado aos seus detector motores de antivírus & e antispyware. O BitDefender é agora capaz de detectar rootkits ao procurar ficheiros, pastas ou processos ocultos. Mais ainda, pode proteger o seu sistema ao renomear o malware que usa os rootkits.

De forma a analisar o seu computador em busca de rootkits, execute a tarefa **Analisar em busca de Rootkits**. Irá aparecer uma janela de análise.

Importante

Quando analisa em busca de rootkits, é fortemente recomendado que defina o BitDefender para não levar a cabo nenhuma acção sobre ficheiros ocultos.

No final da análise poderá ver os resultados. Se tiverem sido detectados ficheiros ocultos, verifique-os cuidadosamente: a presença de ficheiros ocultos poderá indicar uma possível intrusão.

Se tem a certeza de ter detectado ficheiros que pertencem a malware, recomendamos que defina a acção **Renomear ficheiros** e execute novamente a tarefa **Analisar em busca de Rootkits**. Desta forma os ficheiros ocultos serão bloqueados.

Atenção

NEM TODOS OS FICHEIROS OCULTOS SÃO MALWARE! Antes de renomear ficheiros ocultos, certifique-se que eles não pertencem a uma aplicação válida nem ao seu sistema. Renomear tais ficheiros poderá tornar o seu sistema incapaz de funcionar.

Importante

Se o seu sistema foi sujeito a intrusão, só há uma única forma de se livrar completamente da intrusão: reinstalar o seu sistema.

7.3. Quarentena

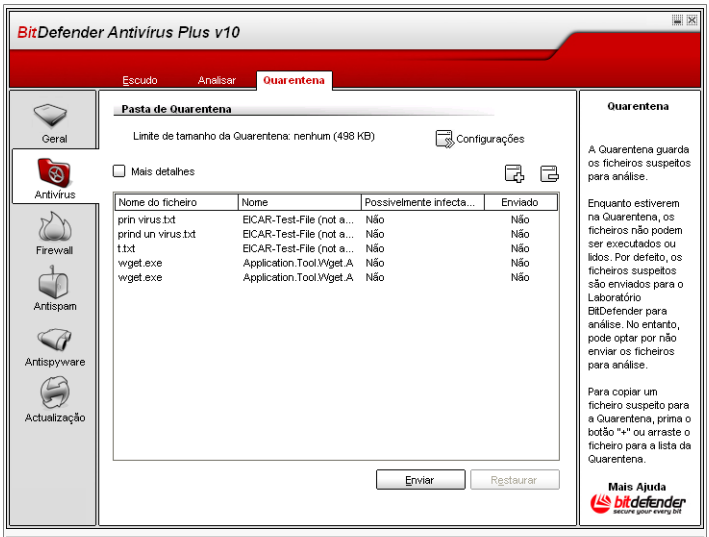

Figura 7.15. Quarentena

O BitDefender permite o isolamento de ficheiros infectados ou suspeitos numa área segura, chamada de quarentena. Ao isolar estes ficheiros na quarentena, desaparece o risco de infecção,e ao mesmo tempo, terá a possibilidade de enviar estes ficheiros para análise no laboratório do BitDefender.

A componente que assegura a administração dos ficheiros isolados é a **Quarentena**. Este módulo foi desenhado com a função de enviar automaticamente os ficheiros infectados para o laboratório do BitDefender.

Como pode ver, a secção da **Quarentena** contém uma lista de todos os ficheiros isolados até então. Todo o ficheiro tem incluído o seu nome, tamanho, data de isolamento e de submissão. Se pretende ver mais informação acerca dos ficheiros na quarentena, clique em **Mais detalhes**.

Nota

Quando o vírus se encontra na quarentena não pode provocar nenhum mal, porque não podem ser lidos nem executados.

Clique no botão **Adicionar** para adicionar à quarentena um ficheiro que suspeita de estar infectado. Uma janela irá abrir e pode seleccionar o ficheiro na sua localização no disco. Desta forma o ficheiro é copiado para a quarentena. Se pretende mover o ficheiro para a zona de quarentena, tem de seleccionar a caixa de selecção correspondente a **Apagar do local de origem**. Um método mais rápido para adicionar ficheiros suspeitos à quarentena, é fazer drag&drop do ficheiro na lista da quarentena.

Para apagar um ficheiro seleccionado da lista de quarentena clique no botão **Remover** . Se deseja restaurar o ficheiro seleccionado para a sua localização original clique em **Restaurar**.

Pode enviar qualquer ficheiro seleccionado da quarentena para os Laboratórios BitDefender clicando no botão **Enviar**.

Importante

Tem de especificar alguma informação antes de enviar estes ficheiros. Para isso clique em **Configuração** e complete os campos da secção das **Configuração de envio**, como descritas abaixo.

Clique em **Configuração** para abrir as opções avançadas da zona de quarentena. Uma nova janela irá aparecer.

As opções da quarentena estão agrupadas em duas categorias:

- **Configuração da quarentena**
- **Configuração de envio**

Nota

Clique na caixa com o "+" para abrir uma opção, ou na caixa com o "-" para fechar uma opção.

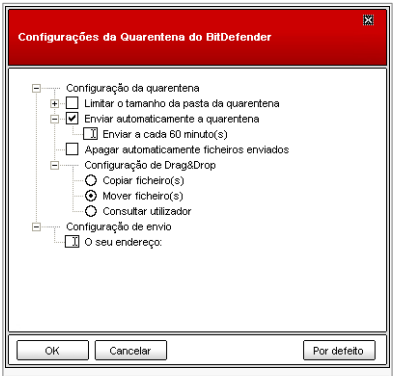

Figura 7.16. Configuração da quarentena

Configuração da quarentena

- **Limitar o tamanho da pasta da quarentena** - mantém o tamanho da quarentena sob controlo. O seu tamanho por defeito é de 12000 KB. Se deseja alterar este valor insira um novo no campo correspondente.

  Se seleccionar a caixa de selecção correspondente a **Apagar automaticamente ficheiros antigos**, quando adicionar um novo ficheiro e a quarentena estiver cheia, os ficheiros mais antigos da quarentena serão apagados automaticamente de modo a libertar espaço para os novos ficheiros.

Nota

Por defeito, a pasta da quarentena não tem limite de tamanho.

- **Enviar automaticamente da quarentena** - envia automaticamente os ficheiros da quarentena para os laboratórios do BitDefender para uma análise posterior. Pode estabelecer o período de tempo, entre dois processos de envio consecutivos, em minutos no campo **Enviar a cada x minutos**.
- **Eliminar automaticamente ficheiros enviados** - elimina automaticamente os ficheiros enviados da quarentena, após o seu envio para análise nos Laboratório do BitDefender.
- **Configuração de Drag & Drop** - se está a usar o método Drag & Drop para adicionar ficheiros à quarentena, aqui poderá especificar a acção: Copiar, mover, ou solicitar ao utilizador.

Configuração de envio

- **O seu endereço** - introduza o seu endereço de e-mail, no caso de desejar receber um e-mail dos nossos especialistas, relativamente aos ficheiros suspeitos que nos enviou para análise.

Clique em **OK** para guardar as alterações Se clicar em **Por defeito** irá carregar as definições por defeito.

Capítulo 8. Módulo Firewall

A secção da **Firewall** deste guia do utilizador contém os seguintes tópicos:

- Estado da Firewall
- Protecção de Tráfego

Nota

Para mais detalhes com respeito ao módulo **Firewall** verifique a descripção do "*Módulo Firewall*" (p. 27).

8.1. Estado da Firewall

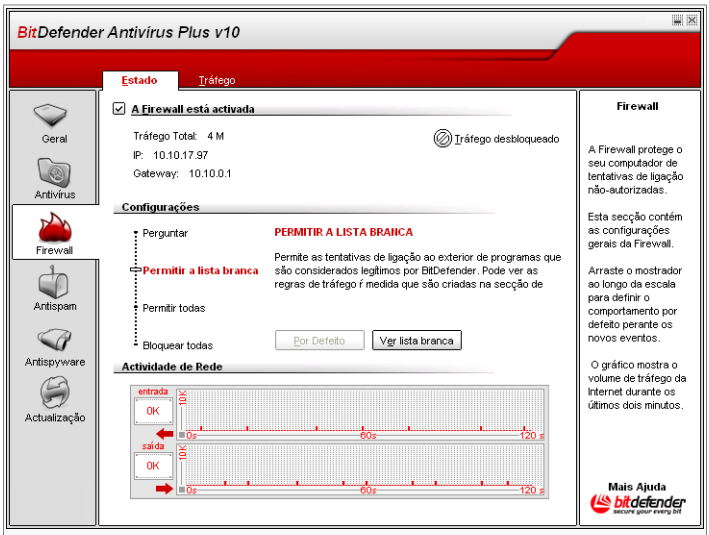

Figura 8.1. Estado da Firewall

Nesta secção pode activar/desactivar a **Firewall**, bloquear todo o tráfego de rede/internet e definir o comportamento por defeito da mesma em novos eventos.

Importante

Para se manter protegido contra os ataques da Internet, mantenha activa a **Firewall**.

Para bloquear toda a rede / Tráfego Internet clique em **Bloquear Tráfego** e depois escolha **Sim** para confirmar a sua opção. Isto irá isolar o seu computador de qualquer outro computador na rede.

Para desbloquer o tráfego mais tarde, basta clicar em **Desbloquear Tráfego**.

Ao fundo e ao lado desta secção pode ver as estatísticas do BitDefender com respeito ao tráfego de entrada e de saída. O gráfico mostra-lhe o volume de tráfego da Internet durante os últimos dois minutos.

Nota

O gráfico aparece mesmo que a **Firewall** esteja desactivada.

8.1.1. Nível de Protecção

Pode escolher o nível de protecção que melhor se adapta às suas necessidades de segurança. Arraste o marcador ao longo da escala para definir o nível de segurança apropriado.

Existem 4 níveis de protecção:

Nível de Protecção	Descrição
Bloquear Todos	Rejeita tentativas de tráfego que não coincidem com nenhumas das regras criadas sem perguntar. Use esta politica se já definiu todas as regras para todos os programas e ligações que necessita.
Permitir Todos	Autoriza as tentativas de ligação que não correspondem às regras actuais. Esta política é muito desaconselhada, mas poderá ser útil para administradores de redes.
Permitir Lista Branca	Permite todas as ligações de saída de programas que o BitDefender considera legítimos. Pode ver as regras à medida que são criadas na secção Tráfego. Programas da Lista Branca são as aplicações mais usadas e comuns a nível mundial. Incluem os mais conhecidos web browsers, audio&video players, programas de chat e filesharing, como também as aplicações de cliente servidor e do sistema operativo.
Perguntar	Perguntar se tentativas de tráfego que não correspondem com nenhuma das regras actuais devem ser permitidas.

Importante

Se a consola de administração é fechada e não foi descoberta qualquer correspondência no conjunto de regras para o novo evento, a acção será **Bloquear**.

Clique em **Nível por Defeito** para definir a política por defeito(**Permitir Lista Branca**).

Se deseja ver quais são os programas da Lista Branca, clique em **Ver Lista Branca**.

8.2. Controlo de Tráfego

BitDefender Antivirus Plus v10
Estado
Tráfego
Geral
Antivírus
Firewall
Antispam
Antispyware
Actualização
Configurações da Firewall:
Programas bloqueados: 1
Nome da Aplicação
Tipo
Direcção
Acção
Aplicação
BitDefender wizar... TCP/UDP Ambos Permitir c:\program files\soft...
Open Computers a... TCP/UDP Ambos Permitir c:\ocs-ng\ocsinvent...
Yahoo! Messenger TCP/UDP Ambos Permitir c:\program files\yah...
Userinit Logon Ap... TCP/UDP Ambos Permitir c:\windows\system...
Yahoo Auto Updater TCP/UDP Ambos Permitir c:\program files\yah...
Firefox TCP/UDP Ambos Permitir c:\program files\moz...
Microsoft Office O... TCP/UDP Ambos Permitir c:\program files\micr...
Internet Explorer TCP/UDP Ambos Permitir c:\program files\inter...
Qualquer TCP/UDP Ambos Bloquear Qualquer
Guardar regras
Carregar regras
Aplicar
Tráfego
The rules are listed in the order of priority, from the top. All the rules are fully customizable. You can permit/deny incoming or outgoing connections, on all or on specific ports and addresses.
Only allowing access to the internet to programs you explicitly trust will greatly improve your system's security.
Tip: Allow inbound connection attempts only from IP's or domains you explicitly trust.
Mais Ajuda
bitdefender

Figura 8.2. Controlo de Tráfego

Nesta secção pode especificar que ligações de entrada e de saída quer permitir/bloquear, ao criar regras para protocolos específicos, portas, aplicações e/ou endereços remotos. Pode também guardar e carregar os conjuntos de regras a aplicar ao tráfego de rede/internet.

As regras podem ser introduzidas automaticamente (através da janela de alerta) ou manualmente (clique no botão **Adicionar** e escolha os parâmetros para a regra).

8.2.1. Adicionar Regras Automaticamente

As regras são adicionadas à lista quando responde às perguntas do BitDefender acerca de um novo programa que tenta aceder à Internet.

Com a **Firewall** activa, o BitDefender irá pedir a sua permissão, sempre que um novo programa tente enviar ou receber informação para e da Internet:

Figura 8.3. Alerta da Firewall BitDefender

Pode visualizar o seguinte: a aplicação que tenta aceder à internet, o endereço de IP e a porta, na qual a aplicação está a tentar conectar-se.

Seleccione a opção **Memorizar esta resposta** e clique em **Sim** ou **Não**, e é criada uma nova regra, que é aplicada e listada na tabela de regras. Desta forma não será novamente notificado quando o processo se repetir.

Importante

Permitir tentativas de ligação apenas de IP's ou domínios em que confia totalmente.

As regras são adicionadas à lista quando responde às perguntas do BitDefender acerca de um novo programa que tenta aceder à Internet.

Cada uma das regras que foi memorizada pode ser acedida na secção de **Tráfego** para posterior afinamento.

8.2.2. Adicionar Regras Manualmente

Clique no botão **Adicionar regra** para dar início ao assistente de configuração.

O assistente de configuração é um procedimento com 4 passos.

Passo 1/4 - Seleccione a Aplicação e a Acção

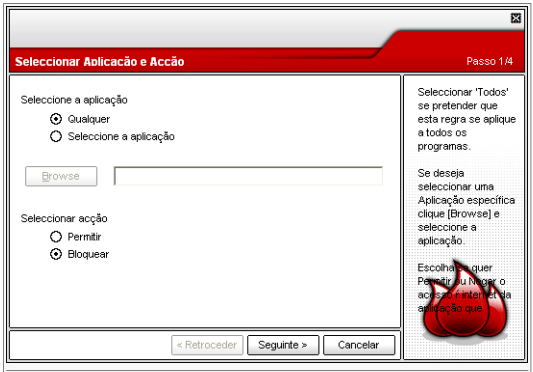

Figura 8.4. Seleccionar Aplicação e Acção

Pode definir os parâmetros:

- **Aplicação** - selecciona a aplicação para a regra. Pode escolher apenas uma aplicação (clique em **Seleccionar aplicação**, em seguida **Explorar** e seleccione a aplicação) ou todas as aplicações (basta clicar em **Todas**).
- **Acção** - selecciona a acção da regra.

Acção	Descrição
Permitir	A acção será permitida.
Bloquear	A acção será negada.

Clique em **Seguinte**.

Passo 2/4 - Seleccionar Portas

Figura 8.5. Seleccionar Portas

Está disponível uma lista com as portas mais comuns e uma breve descrição para ajudá-lo a seleccionar apenas portas específicas. Clique em **Especificar porta(s)**, escolha as portas, nas quais a regra será aplicada e clique em **Adicionar**.

Se seleccionou **Todas**, todas as portas serão seleccionadas. Se deseja eliminar uma porta, basta seleccioná-la e clicar em **Remover**.

Clique em **Seguinte**.

Passo 3/4 - Seleccionar Endereços de IP

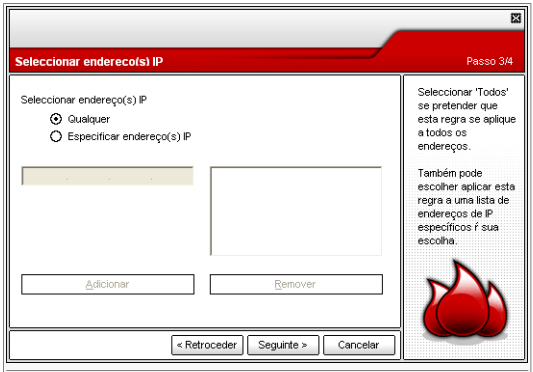
Seleccionar endereco(s) IP
Passo 3/4
Seleccionar endereço(s) IP
Qualquer
Especificar endereço(s) IP
Adicionar
Remover
« Retroceder
Seguinte »
Cancelar
Seleccionar 'Todos' se pretender que esta regra se aplique a todos os endereços.
Também pode escolher aplicar esta regra a uma lista de endereços de IP específicos à sua escolha.

Figura 8.6. Seleccionar Endereços de IP

Clique em **Especificar endereço(s) de IP**, introduza os endereços de IP, nos quais a regra será aplicada e clique em **Adicionar**.

Seleccione **Todos** se deseja que esta regra se aplique a todos os endereços de IP. Para eliminar um endereço de IP, basta seleccioná-lo e clicar em **Remover**.

Clique em **Seguinte**.

Passo 4/4 - Seleccionar Tipo e Direcção

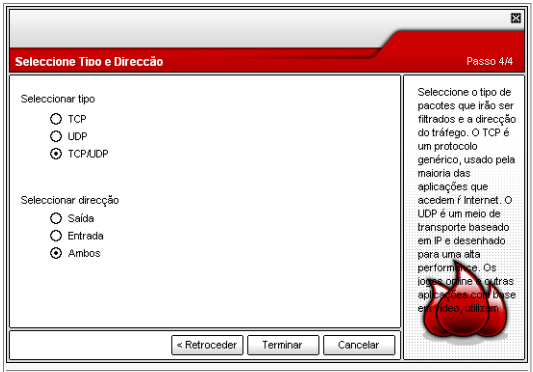
Seleccione Tipo e Direcção
Passo 4/4
Seleccionar tipo
TCP
UDP
TCP/UDP
Seleccionar direcção
Saída
Entrada
Ambos
Seleccione o tipo de pacotes que irão ser filtrados e a direcção do tráfego. O TCP é um protocolo genérico, usado pela maioria das aplicações que acedem à Internet. O UDP é um meio de transporte baseado em IP e desenhado para uma alta performance. Os jogos online e outras aplicações com base em vídeo, utilizam
< Retroceder
Terminar
Cancelar

Figura 8.7. Seleccionar Tipo e Direcção

Pode definir os parâmetros:

- **Tipo de protocolo** - seleccione os protocolos TCP, UDP ou ambos.

Tipo	Descrição
TCP	Transmission Control Protocol - TCP permite que dois hosts estabeleçam uma ligação e troquem dados entre si. O TCP garante a entrega dos dados e também garante que os pacotes serão entregues na mesma ordem em que foram enviados.
UDP	User Datagram Protocol - UDP é um meio de transporte baseado em IP desenhado para uma elevada performance. Os jogos e outras aplicações baseadas em vídeo usam com frequência o UDP.
TCP/UDP	Transmission Control Protocol e User Datagram Protocol.

- **Sentido** - selecciona o sentido do tráfego.

Tipo	Descrição
Saída	A regra aplica-se apenas ao tráfego de saída.
Entrada	A regra aplica-se apenas ao tráfego de entrada.
Ambos	A regra aplica-se em ambos os sentidos.

Clique em **Terminar**.

Clique em **Aplicar** para guardar as alterações.

Capítulo 9. Módulo Antispam

A secção do **Antispam** deste guia do utilizador contém os seguintes tópicos:

- Estado do Antispam
- Configurações de Antispam
- Integração com o Microsoft Outlook / Outlook Express / Windows Mail

Nota

Para mais detalhes com respeito ao módulo **Antispam** verifique a descripção do "*Módulo Antispam*" (p. 28).

9.1. Estado do Antispam

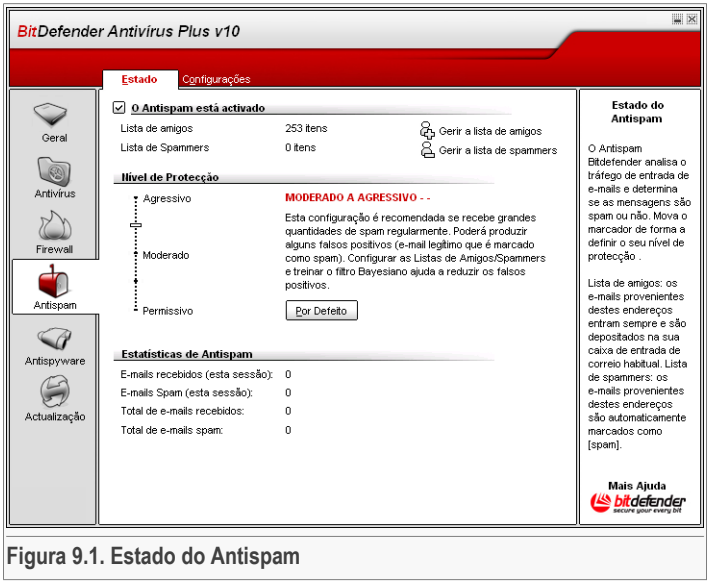
BitDefender Antivírus Plus v10
Estado
Configurações
Geral
Antivírus
Firewall
Antispam
Antispyware
Actualização
O Antispam está activado
Lista de amigos
253 itens
Gerir a lista de amigos
Lista de Spammers
0 itens
Gerir a lista de spammers
Nível de Protecção
Agressivo
Moderado
Permissivo
MODERADO A AGRESSIVO - -
Esta configuração é recomendada se recebe grandes quantidades de spam regularmente. Poderá produzir alguns falsos positivos (e-mail legítimo que é marcado como spam). Configurar as Listas de Amigos/Spammers e treinar o filtro Bayesiano ajuda a reduzir os falsos positivos.
Por Defeito
Estatísticas de Antispam
E-mails recebidos (esta sessão): 0
E-mails Spam (esta sessão): 0
Total de e-mails recebidos: 0
Total de e-mails spam: 0
Estado do Antispam
O Antispam Bitdefender analisa o tráfego de entrada de e-mails e determina se as mensagens são spam ou não. Mova o marcador de forma a definir o seu nível de protecção .
Lista de amigos: os e-mails provenientes destes endereços entram sempre e são depositados na sua caixa de entrada de correio habitual. Lista de spammers: os e-mails provenientes destes endereços são automaticamente marcados como [spam].
Mais Ajuda
bitdefender

Figura 9.1. Estado do Antispam

Nesta secção pode configurar o módulo de **Antispam** e pode visualizar informação acerca da sua actividade.

Importante

Para prevenir a entrada de Spam na sua **Caixa de Entrada**, mantenha activo o **Filtro Antispam**.

Na secção das **Estatísticas** pode visualizar as estatísticas que dizem respeito ao módulo de Antispam. Os resultados são apresentados por sessão (desde que iniciar o seu computador) ou pode ver um sumário da actividade de Antispam desde a instalação do Filtro de Antispam.

Para configurar o módulo de **Antispam** é necessário proceder da seguinte maneira:

9.1.1. Preencher a Lista de Endereços

As listas de endereços contêm informação acerca dos endereços de e-mail que lhe enviam mensagens de e-mail legítimas ou spam.

Lista de Amigos

A **Lista de amigos** é uma lista de todos os endereços de e-mail, dos quais deseja receber mensagens, independentemente do seu conteúdo. As mensagens dos seus amigos não são marcadas como spam, mesmo que o conteúdo se assemelhe a spam.

Nota

Qualquer e-mail proveniente de um endereço presente na **Lista de amigos**, será automaticamente entregue na sua Caixa de Entrada.

Para gerir a **Lista de amigos** clique em (correspondente à **Lista de amigos**) ou clique no botão **Amigos** na Barra de tarefas Antispam.

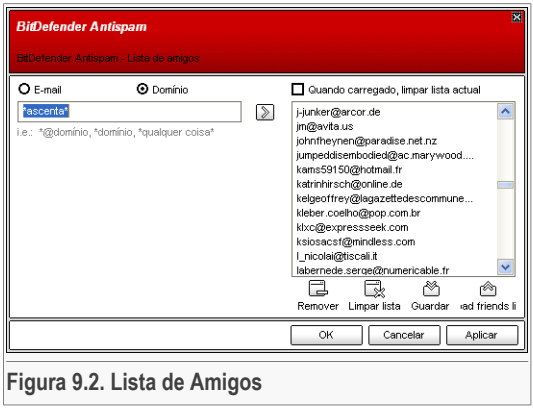

Figura 9.2. Lista de Amigos

Aqui pode adicionar ou remover entradas da **Lista de amigos**.

Se quiser adicionar um endereço de e-mail seleccione a opção **E-mail** introduza-o e clique no botão . O endereço irá aparecer na **Lista de amigos**.

Importante

Sintaxe: <nome@dominio.com>.

Se pretende adicionar um domínio seleccione a opção **Domínio**, introduza-o e clique no botão . O domínio irá aparecer na **Lista de amigos**.

Importante

Sintaxe:

- <@dominio.com>, <*dominio.com> e <dominio.com> - todos os mails provenientes de <dominio.com> chegarão à sua **Caixa de Entrada** independentemente do seu conteúdo;
- <*dominio*> - todos os mails provenientes de <dominio> (sem interessar os sufixos do dominio) chegarão à sua **Caixa de Entrada** independentemente do seu conteúdo;
- <*com> - todos os mails que têm este sufixo de domínio <com> chegarão à sua **Caixa de Entrada** independentemente do seu conteúdo.

Para apagar um item da listas, seleccione-o e clique no botão **Remover** . Se clicar no botão **Limpar lista** , irá apagar todas as entradas da lista, mas atenção: é impossível recuperá-las.

Use os botões **Guardar**/ **Carregar** para guardar / carregar a **Lista de amigos** para/de um local desejado. O ficheiro irá ter a extensão .bwl.

Para fazer reset ao conteúdo da lista actual quando carrega uma lista guardada previamente seleccione **Quando carregar, limpar lista actual**.

Nota

Recomendamos que adicione os nomes e endereços de e-mail dos seus amigos à **Lista de Amigos**. O BitDefender não bloqueia mensagens dos presentes nessa lista; deste modo, a adição de amigos ajuda a assegurar a passagem de mensagens legítimas.

Clique em **Aplicar** e **OK** para guardar e fechar a **Lista de amigos**.

Lista de Spammers

A **Lista de Spammers** é uma lista de todos os endereços de e-mail, dos quais não quer receber mensagens, independentemente do seu conteúdo.

Nota

Todo o e-mail proveniente de um endereço presente na **Lista de Spammers**, será marcado automaticamente como SPAM.

Para gerir a **Lista de spammers** clique em (correspondente à **Lista de spammers**) ou clique no botão **Spammers** na Barra de tarefas Antispam.

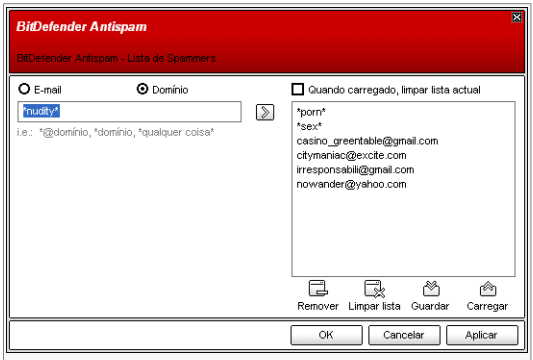

Figura 9.3. Lista de Spammers

Aqui pode adicionar ou remover entradas da **Lista de Spammers**.

Se quiser adicionar um endereço de email seleccione a opção **E-mail**, insira o endereço e clique no botão . O endereço irá aparecer na **Lista de spammers** .

Importante

Sintaxe: `<nome@dominio.com>`.

Se pretende adicionar um domínio seleccione a opção**Domínio**, insira-o e clique no botão . O domínio irá aparecer na **Lista de spammers**.

Importante

Sintaxe:

- `<@dominio.com>`, `<*dominio.com>` e `<dominio.com>` - todos os e-mails provenientes de `<dominio.com>` serão marcados como SPAM;

- <*dominio*> - todos os e-mails provenientes de <dominio> (independentemente dos sufixos de domínio) serão marcados como SPAM;
- <*com> - todos os e-mails tendo o sufixo de domínio <com> serão marcados como SPAM.

Para apagar um item da listas, seleccione-o e clique no botão **Remover** . Se clicar no botão **Limpar lista** , irá apagar todas as entradas da lista, mas atenção: é impossível recuperá-las.

Use os botões **Guardar**/ **Carregar** para guardar / carregar a **Lista de spammers** para/de o local desejado. O ficheiro terá a extensão .bwl.

Para fazer reset ao conteúdo da lista actual quando carrega uma lista guardada previamente seleccione **Quando carregar, limpar lista actual**.

Clique em **Aplicar** e **OK** para guardar e fechar a **Lista de Spammers**.

Importante

Se deseja reinstalar o BitDefender será uma boa ideia guardar as listas de **Amigos** / **Spammers**, antes do processo de reinstalação, e após o processo de reinstalação ter terminado pode carregá-las.

9.1.2. Definir o Nível de Tolerância

Pode escolher o nível de protecção que melhor se adapta às suas necessidades de segurança. Arraste o marcador ao longo da escala para definir o nível de segurança apropriado.

Existem 5 níveis de tolerância:

Nível de Tolerância	Descrição
Tolerante	Oferece protecção às contas que recebem uma grande quantidade de e-mails comerciais legítimos. O filtro irá deixar passar a maior parte dos e-mails, mas poderá produzir falsos negativos (spam classificado como e-mail legítimo).
Tolerante a Moderado	Oferece protecção às contas que recebem alguns e-mails comerciais legítimos. O filtro irá deixar passar a maior parte dos e-mails, mas poderá produzir falsos negativos (spam classificado como e-mail legítimo).

Nível de Tolerância	Descrição
Moderado	Oferece protecção às contas regulares. O filtro bloqueará a maioria do spam, enquanto evita falsos positivos.
Moderado a Agressivo	Oferece protecção às contas que recebem uma grande quantidade de spam regularmente. O filtro irá deixar passar muito pouco spam, mas produzirá falsos positivos (e-mail legítimo marcado incorrectamente como spam). Configura as **Listas de Amigos/Spammers** e treina o **Motor de Aprendizagem (Bayesiano)** de forma a reduzir o número de falsos positivos.
Agressivo	Oferece protecção a contas que recebem um volume muito elevado de spam regularmente. O filtro irá deixar passar muito pouco spam, mas produzirá falsos positivos (e-mail legítimo marcado incorrectamente como spam). Adicione os seus contactos à **Lista de Amigos** de forma a reduzir o número de falsos positivos.

Para definir o nível de protecção por defeito (**Moderado a Agressivo**) clique em **Nível por Defeito**.

9.2. Configurações de Antispam

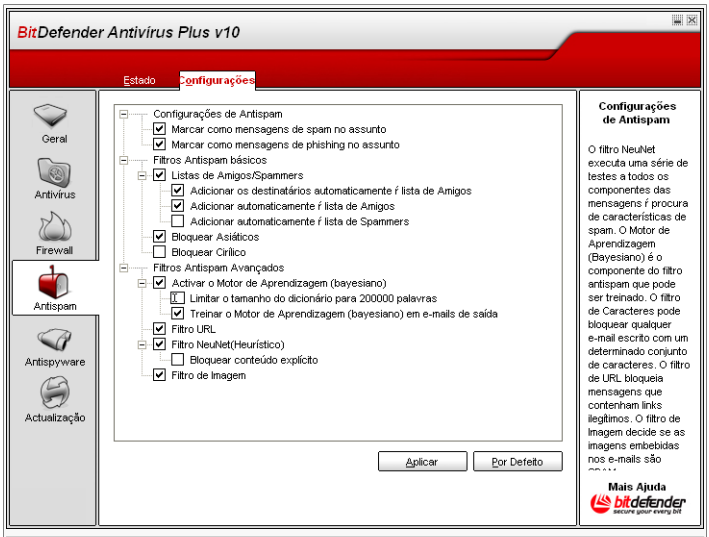
BitDefender Antivírus Plus v10
Estado
Configurações
Geral
Antivírus
Firewall
Antispam
Antispyware
Actualização
Configurações de Antispam
Marcar como mensagens de spam no assunto
Marcar como mensagens de phishing no assunto
Filtros Antispam básicos
Listas de Amigos/Spammers
Adicionar os destinatários automaticamente à lista de Amigos
Adicionar automaticamente à lista de Amigos
Adicionar automaticamente à lista de Spammers
Bloquear Asiáticos
Bloquear Cirílico
Filtros Antispam Avançados
Activar o Motor de Aprendizagem (bayesiano)
Limitar o tamanho do dicionário para 200000 palavras
Treinar o Motor de Aprendizagem (bayesiano) em e-mails de saída
Filtro URL
Filtro NeuNet(Heurístico)
Bloquear conteúdo explícito
Filtro de Imagem
Aplicar
Por Defeito
Configurações de Antispam
O filtro NeuNet executa uma série de testes a todos os componentes das mensagens à procura de características de spam. O Motor de Aprendizagem (Bayesiano) é o componente do filtro antispam que pode ser treinado. O filtro de Caracteres pode bloquear qualquer e-mail escrito com um determinado conjunto de caracteres. O filtro de URL bloqueia mensagens que contenham links ilegítimos. O filtro de Imagem decide se as imagens embebidas nos e-mails são
Mais Ajuda
bitdefender

Figura 9.4. Configurações de Antispam

Aqui pode activar/desactivar cada um dos filtros Antispam e pode especificar outras definições com respeito ao módulo Antispam.

Encontram-se disponíveis três categorias de opções (**Configuração de Antispam**, **Filtros básicos de Antispam** e **Filtros avançados de Antispam**) organizadas num menu expansível, semelhante aos do Windows.

Nota

Clique na caixa marcada com o sinal "+" para abrir a categoria ou clique na que está marcada com o sinal "-" para fechar a categoria.

9.2.1. Configurações de Antispam

- **Marcar como mensagem de spam no assunto** - todas as mensagens de e-mail consideradas spam serão marcadas como SPAM no assunto.
- **Marcar mensagens phishing no assunto** - todas as mensagens de e-mail consideradas mensagens de phishing serão marcadas como SPAM na linha do assunto.

9.2.2. Filtros Antispam Básicos

- **Listas de amigos / spammers** - activa/desactiva as Listas de amigos / spammers;
  - **Adicionar automaticamente à lista de Amigos** - para adicionar os destinatários de e-mails enviados à Lista de Amigos.
  - **Adicionar automaticamente à Lista de amigos** - da próxima vez que clicar no botão **Não-Spam** na Barra de tarefas Antispamo remetente será automaticamente adicionado à **Lista de amigos**.
  - **Adicionar automaticamente à Lista de Spammers** - da próxima vez que clicar no botão **É Spam** na Barra de tarefas Antispam o remetente será automaticamente adicionado à **Lista de Spammers**.

Nota
Os botões **Não-Spam** e **É Spam** são usados para treinar o filtro Bayesiano.

- **Bloquear Asiático** - bloqueia mensagens escritas com Caracteres asiáticos.
- **Bloquear Cirílico** - bloqueia mensagens escritas com Caracteres cirílicos.

9.2.3. Filtros Antispam Avançados

- **Activar Motor de Aprendizagem (bayesiano)** - activa/desactiva o Motor de Aprendizagem (bayesiano);
  - **Limitar o tamanho do dicionário para 200000 palavras** - com esta opção pode estabelecer o tamanho do dicionário Bayesian – quanto menor mais rápido, maior é mais eficaz.

Nota
O tamanho recomendado é de: 200.000 palavras.

  - **Treinar Motor de Aprendizagem (bayesiano) nos e-mails de saída** - treina o Motor de Aprendizagem (bayesiano) nos e-mails de saída.
- **Filtro URL** - activa/desactiva o Filtro URL;
- **Filtro NeuNet (Heurístico)** - activa/desactiva o Filtro NeuNet (Heurístico);
  - **Bloquear conteúdo explícito** - activa/desactiva a detecção de mensagens com o aviso de conteúdo SEXUALMENTE EXPLÍCITO na linha do assunto.
- **Filtro de Imagem** - activa/desactiva o Filtro de Imagem.

Nota

Para activar/desactivar uma opção seleccione/limpe a caixa de selecção correspondente a ela.

Clique em **Aplicar** para guardar as alterações, ou clique em **Nível por Defeito** para carregar as definições por defeito.

9.3. Integração como o Microsoft Outlook / Outlook Express / Windows Mail

BitDefender integra-se directamente com o Microsoft Outlook / Outlook Express / Windows Mail através de uma barra de tarefas intuitiva e fácil de usar.

9.3.1. Barra de Ferramentas do Antispam

No lado superior do Microsoft Outlook / Outlook Express/ Windows Mail pode ver a barra de ferramentas do Antispam .

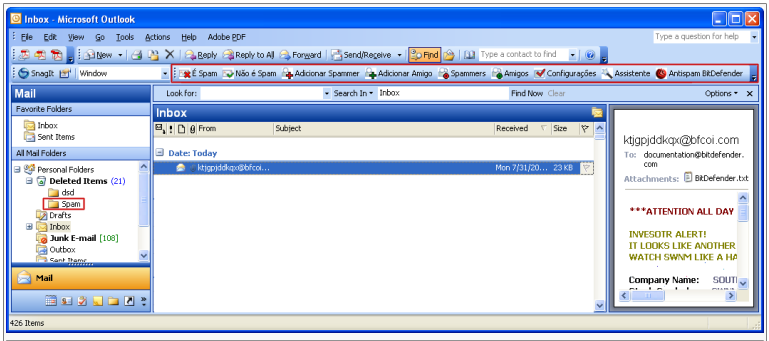

Figura 9.5. Barra de Ferramentas do Antispam

Importante

A diferença entre o BitDefender Antispam para o Microsoft Outlook e o do Outlook Express/ Windows Mail, é que as mensagens SPAM são movidas para a pasta de **Spam** para o Microsoft Outlook e no Outlook Express elas são movidas para a pasta **Itens Eliminados**. Em ambos os casos as mensagens são marcadas como SPAM, na linha do assunto.

A pasta de **Spam** é criada automaticamente pelo BitDefender no Microsoft Outlook e é listada ao mesmo nível com os itens da **Lista de Pastas**(Calendário, Contactos, etc).

Cada botão da barra de tarefas BitDefender é explicado abaixo:

- **É Spam** - envia uma mensagem ao módulo Bayesiano, indicando que o e-mail seleccionado é spam. O e-mail será marcado como SPAM e será movido para a pasta de **Spam**.

  As futuras mensagens de e-mail que se enquadrem no mesmo padrão serão marcadas como SPAM.

  Nota
  Pode seleccionar uma mensagem de e-mail ou tantas quantas desejar.

- **Não é Spam** - envia uma mensagem ao módulo Bayesiano, indicando que o e-mail seleccionado não é spam, e que o BitDefender não o deve marcar como tal. O e-mail será movido da pasta de **Spam** para o directório da **Caixa de Entrada**.

  As futuras mensagens de e-mail que se enquadrem no mesmo padrão não serão marcadas como SPAM.

  Nota
  Pode seleccionar uma mensagem de e-mail ou tantas quantas desejar.

  Importante
  O botão **Não é Spam** fica activo quando seleccionar uma mensagem marcada como SPAM pelo BitDefender (normalmente estas mensagens localizam-se na pasta de **Spam**).

- **Adicionar spammer** - adiciona o remetente da mensagen seleccionada à **Lista de Spammers**.

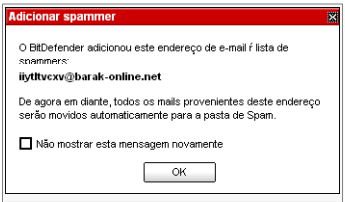
Adicionar spammer
O BitDefender adicionou este endereço de e-mail í lista de spammers:
iiyttlvcxv@barak-online.net
De agora em diante, todos os mails provenientes deste endereço serão movidos automaticamente para a pasta de Spam.
Não mostrar esta mensagem novamente
OK

Figura 9.6. Adicionar Spammer

Seleccione **Não mostrar esta mensagem novamente** se não quer ser consultado para confirmação, quando adiciona à lista um endereço de um spammer.

Clique em **OK** para fechar a janela.

As futuras mensagens de e-mail provenientes desses endereços serão marcadas como SPAM.

Nota

Pode seleccionar um remetente ou tantos quantos desejar.

- **Adicionar Amigo** - adiciona o remetente das mensagens seleccionadas à sua **Lista de Amigos**.

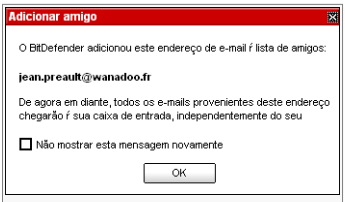
Adicionar amigo
O BitDefender adicionou este endereço de e-mail í lista de amigos:
jean.preault@wanadoo.fr
De agora em diante, todos os e-mails provenientes deste endereço chegarão í sua caixa de entrada, independentemente do seu
Não mostrar esta mensagem novamente
OK

Figura 9.7. Adicionar Amigo

Seleccione **Não mostrar esta mensagem novamente** se não quer ser consultado para confirmação, quando adiciona à lista um endereço amigo.

Clique em **OK** para fechar a janela.

Irá sempre receber mensagens de e-mail destes endereços, independentemente do conteúdo dos mesmos.

Nota

Pode seleccionar um remetente ou tantos quantos desejar.

- **Spammers** - abre a **Lista de Spammers** que contém todos os endereços de e-mail dos quais não deseja receber mensagens de e-mail, independentemente do seu conteúdo.

Nota

Todo o e-mail proveniente de um endereço presente na **Lista de Spammers**, será marcado automaticamente como SPAM.

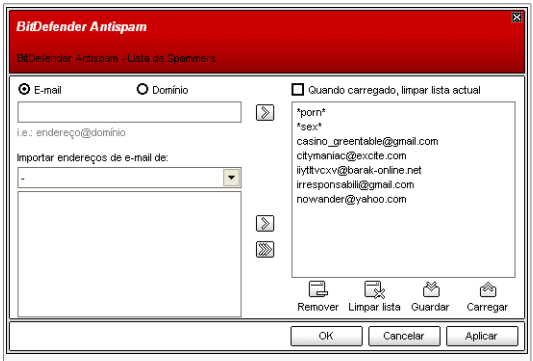

Figura 9.8. Lista de Spammers

Aqui pode adicionar ou remover entradas da **Lista de Spammers**.

Se pretender adicionar um endereço de e-mail seleccione a opção **E-mail**, introduza-o e clique no botão . Os endereços irão aparecer na **Lista de Spammers**.

Importante

Sintaxe: `<nome@dominio.com>`.

Se pretende adicionar um domínio seleccione a opção **Domínio**, introduza-o e clique em . O domínio irá aparecer na **Lista de Spammers**.

Importante

Sintaxe:

- `<@dominio.com>`, `<*dominio.com>` e `<dominio.com>` - todos os e-mails provenientes de `<dominio.com>` serão marcados como SPAM;
- `<*dominio*>` - todos os e-mails provenientes de `<dominio>` (independentemente dos sufixos de domínio) serão marcados como SPAM;
- `<*com>` - todos os e-mails tendo o sufixo de domínio `<com>` serão marcados como SPAM.

Para importar endereços de e-mail de **Livro de Endereços do Windows**/**Pastas do Outlook Express** para o **Microsoft Outlook**/**Outlook Express** / **Windows Mail** seleccione a opção apropriada do menu expansível**Importar endereços de e-mail de**.

Para o **Microsoft Outlook Express/ Windows Mail** aparecerá uma nova janela de onde poderá seleccionar a pasta que contém os endereços de e-mail que deseja adicionar à **Lista de spammers**. Escolha-os e clique em **Seleccionar**.

Em ambos os casos, os endereços de e-mail aparecerão na lista de importação. Seleccione os que deseja e clique em para os adicionar à **Lista de Spammers**. Se clicar em todos os endereços de e-mail serão adicionados à lista.

Para apagar um item da listas, seleccione-o e clique no botão **Remover** . Se clicar no botão **Limpar lista** , irá apagar todas as entradas da lista, mas atenção: é impossível recuperá-las.

Use os botões **Guardar**/ **Carregar** para guardar / carregar a **Lista de spammers** para/de o local desejado. O ficheiro terá a extensão `.bwl`.

Para fazer reset ao conteúdo da lista actual quando carrega uma lista guardada previamente seleccione **Quando carregar, limpar lista actual**.

Clique em **Aplicar** e **OK** para guardar e fechar a **Lista de Spammers**.

- **Amigos** - abre a **Lista de amigos** que contém todos os endereços de e-mail dos quais deseja receber mensagens de e-mail, independentemente do seu conteúdo.

Nota

Qualquer e-mail proveniente de um endereço presente na **Lista de amigos**, será automaticamente entregue na sua Caixa de Entrada.

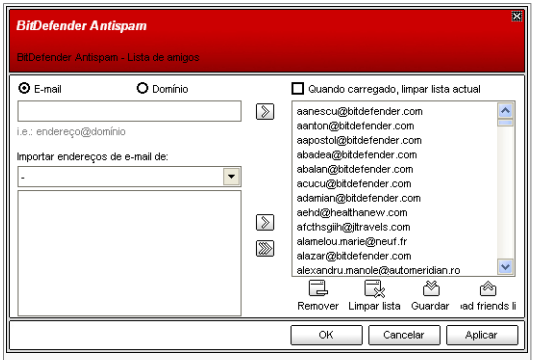

Figura 9.9. Lista de Amigos

Aqui pode adicionar ou remover entradas da **Lista de amigos**.

Se pretender adicionar um endereço de e-mail seleccione a opção **E-mail**, insira-o e clique no botão . O endereço irá aparecer na **Lista de amigos**.

Importante

Sintaxe: `<nome@dominio.com>`.

Se pretende adicionar um domínio seleccione a opção **Domínio**, introduza-o e clique em . O domínio irá aparecer na **Lista de amigos**.

Importante

Sintaxe:

- `<@dominio.com>`, `<*dominio.com>` e `<dominio.com>` - todos os mails provenientes de `<dominio.com>` chegarão à sua **Caixa de Entrada** independentemente do seu conteúdo;
- `<*dominio*>` - todos os mails provenientes de `<dominio>` (sem interessar os sufixos do dominio) chegarão à sua **Caixa de Entrada** independentemente do seu conteúdo;
- `<*com>` - todos os mails que têm este sufixo de domínio `<com>` chegarão à sua **Caixa de Entrada** independentemente do seu conteúdo.

Para importar endereços de e-mail de **Livro de Endereços do Windows**/**Pastas do Outlook Express** para o **Microsoft Outlook**/**Outlook Express** / **Windows Mail** seleccione a opção apropriada do menu expansível**Importar endereços de e-mail de**.

Para o **Microsoft Outlook Express / Windows Mail** aparecerá uma nova janela onde poderá seleccionar a pasta que contém os endereços de e-mail que deseja adicionar à **Lista de Amigos**. Escolha-os e clique em **Seleccionar**.

Em ambos os casos, os endereços de e-mail aparecerão na lista de importação. Seleccione os desejados e clique em para os adicionar à **Lista de Amigos**. Se clicar em todos os endereços de e-mail serão adicionados à lista.

Para apagar um item da listas, seleccione-o e clique no botão **Remover** . Se clicar no botão **Limpar lista** , irá apagar todas as entradas da lista, mas atenção: é impossível recuperá-las.

Use os botões **Guardar**/ **Carregar** para guardar / carregar a **Lista de amigos** para/de um local desejado. O ficheiro irá ter a extensão `.bwl`.

Para fazer reset ao conteúdo da lista actual quando carrega uma lista guardada previamente seleccione **Quando carregar, limpar lista actual**.

Nota

Recomendamos que adicione os nomes e endereços de e-mail dos seus amigos à **Lista de Amigos**. O BitDefender não bloqueia mensagens dos presentes nessa lista; deste modo, a adição de amigos ajuda a assegurar a passagem de mensagens legítimas.

Clique em **Aplicar** e **OK** para guardar e fechar a **Lista de amigos**.

- **Configuração** - abre a janela das **Configurações** onde pode definir algumas opções para o módulo **Antispam**.

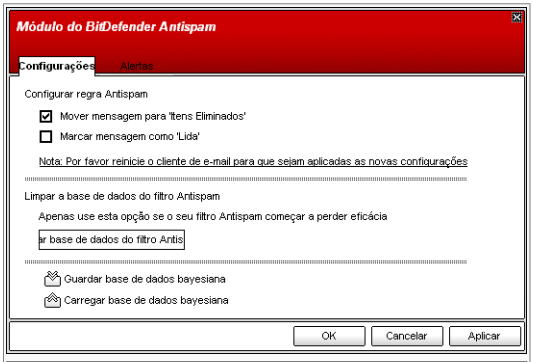
Módulo do BitDefender Antispam
Configurações
Alertas
Configurar regra Antispam
Mover mensagem para 'Itens Eliminados'
Marcar mensagem como 'Lida'
Nota: Por favor reinicie o cliente de e-mail para que sejam aplicadas as novas configurações
Limpar a base de dados do filtro Antispam
Apenas use esta opção se o seu filtro Antispam começar a perder eficácia
ar base de dados do filtro Antis
Guardar base de dados bayesiana
Carregar base de dados bayesiana
OK
Cancelar
Aplicar

Figura 9.10. Configuração

Estão disponíveis as seguintes opções:

- **Mover mensagens para Itens eliminados** - para mover as mensagens de spam para os **Itens eliminados** (apenas para o Microsoft Outlook Express / Windows Mail);
- **Marcar mensagem como 'Lida'** - para marcar todas as mensagens Spam como lidas, para que, quando chegarem novas mensagens spam não seja incomodado.

Se o seu filtro Antispam for muito impreciso, pode necessitar de limpar a base de dados do filtro e voltar a treinar o Filtro Bayesiano. Clique em **Limpar dados do filtro Antispam** se pretende fazer reset à base de dados do filtro Bayesiano.

Utilize os botões **Guardar bayes**/ **Carregar bayes** para guardar/carregar a lista da base de dados Bayesiana para um local desejado. O ficheiro terá uma extensão `.dat`.

Clique no botão **Alertas** se deseja aceder à secção onde poderá desactivar a aparição da janela de confirmação para os botões **Adicionar Spammer** e **Adicionar Amigo**.

Nota

Na janela de **Alertas** pode activar/desactivar a aparição do alerta **Por favor seleccione um e-mail** . Este alerta surge quando selecciona um grupo em vez uma mensagem de e-mail.

- **Assistente** - abre o assistente que irá guiá-lo através do processo de treino do Filtro Bayesiano, para que a eficácia do BitDefender Antispam seja aumentada. Também pode adicionar endereços do seu **Livro de Endereços** à sua **lista de Amigos** / **lista de Spammers**.
- **BitDefender Antispam** - abre a Consola de Administração.

9.3.2. Assistente de Configuração Antispam

A primeira vez que executar o Microsoft Outlook / Outlook Express / Windows Mail com o BitDefender instalado, irá aparecer-lhe um assistente para o ajudar a configurar a Lista de Amigos e a Lista de Spammers e a treinar o Filtro Bayesiano, para aumentar a eficácia dos filtros Antispam.

Nota

O assistente pode ser executado a qualquer altura que deseje clicando no botão **Assistente** na Barra de tarefas Antispam.

Passo 1/6 - Janela de Boas-vindas

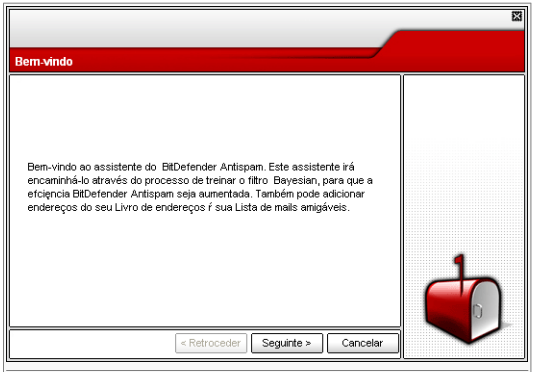
Bem-vindo
Bem-vindo ao assistente do BitDefender Antispam. Este assistente irá encaminhá-lo através do processo de treinar o filtro Bayesian, para que a efciência BitDefender Antispam seja aumentada. Também pode adicionar endereços do seu Livro de endereços í sua Lista de mails amigáveis.
< Retroceder
Seguinte >
Cancelar

Figura 9.11. Janela de boas-vindas

Clique em **Seguinte**.

Passo 2/6 - Preencher a Lista de Amigos

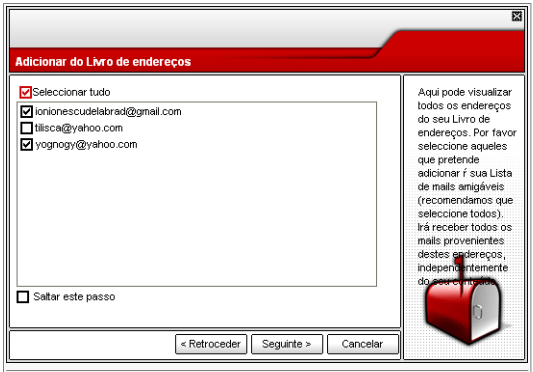
Adicionar do Livro de endereços
Seleccionar tudo
ionionescudelabrad@gmail.com
tilisca@yahoo.com
yognogy@yahoo.com
Saltar este passo
Aqui pode visualizar todos os endereços do seu Livro de endereços. Por favor seleccione aqueles que pretende adicionar à sua Lista de mails amigáveis (recomendamos que seleccione todos). Irá receber todos os mails provenientes destes endereços, independentemente
« Retroceder
Seguinte »
Cancelar

Figura 9.12. Preencher a Lista de Amigos

Aqui pode ver todos os endereços do seu **Livro de Endereços**. Por favor seleccione os que pretende adicionar à sua **Lista de Amigos** (recomendamos que seleccione todos). Irá receber todas as mensagens de e-mail desses endereços, independentemente do seu conteúdo.

Seleccione **Saltar este passo** se pretender omitir este passo. Clique em **Retroceder** para voltar ao passo anterior ou clique em **Seguinte** para continuar.

Passo 3/6 - Apagar a Base de Dados Bayesiana

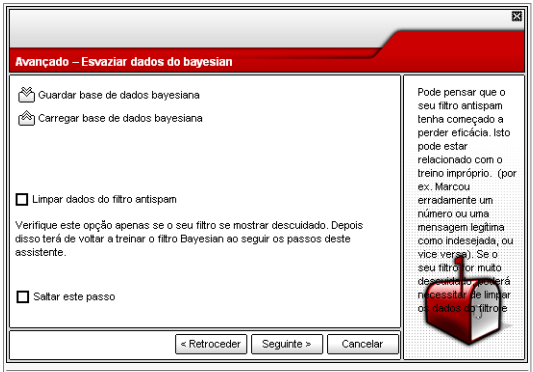
Avançado – Esvaziar dados do bayesian
Guardar base de dados bayesiana
Carregar base de dados bayesiana
Limpar dados do filtro antispam
Verifique este opção apenas se o seu filtro se mostrar descuidado. Depois disso terá de voltar a treinar o filtro Bayesian ao seguir os passos deste assistente.
Saltar este passo
Pode pensar que o seu filtro antispam tenha começado a perder eficácia. Isto pode estar relacionado com o treino impróprio. (por ex. Marcou erradamente um número ou uma mensagem legítima como indesejada, ou vice versa). Se o seu filtro for muito
necessitará de limpar os dados do filtro e
< Retroceder
Seguinte >
Cancelar

Figura 9.13. Apagar a Base de Dados Bayesiana

Poderá deparar-se com o facto do seu filtro de Antispam começado a perder eficácia. Isto pode estar relacionado com treino inapropriado (por ex. por erro, marcou um certo número de mensagens legítimas como spam, ou vice versa). Se o seu filtro for muito impreciso, poderá necessitar de limpar a base de dados e voltar a treinar o filtro seguindo os passos deste assistente.

Seleccione **Limpar dados do filtro Antispam** se pretende efectuar reset à base de dados do filtro Bayesiano.

Utilize os botões **Guardar bayes**/ **Carregar bayes** para guardar/carregar a lista da base de dados Bayesiana para um local desejado. O ficheiro terá uma extensão `.dat`.

Seleccione **Saltar este passo** se pretender omitir este passo. Clique em **Retroceder** para voltar ao passo anterior ou clique em **Seguinte** para continuar.

Passo 4/6 - Treinar o filtro Bayesiano com E-mails Legítimos

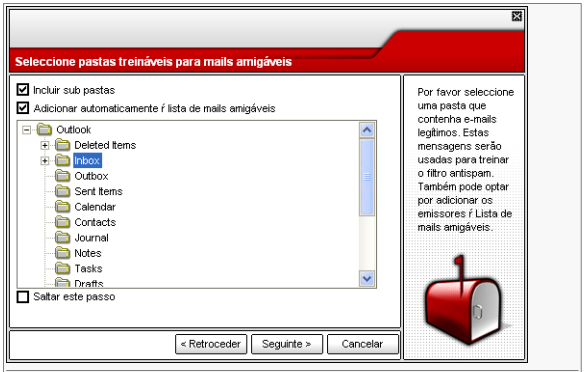

Figura 9.14. Treinar o filtro Bayesiano com E-mails Legítimos

Por favor seleccione a pasta que contém mensagens de e-mail legítimas. Estas mensagens serão usadas para treinar o filtro Bayesiano.

No lado superior da janela estão disponíveis duas opções:

- **Incluir sub-pastas** - para incluir as sub-pastas à sua selecção;
- **Adicionar automaticamente à lista de amigos** - para adicionar os remetentes à **Lista de Amigos**.

Seleccione **Saltar este passo** se pretender omitir este passo. Clique em **Retroceder** para voltar ao passo anterior ou clique em **Seguinte** para continuar.

Passo 5/6 - Treinar o filtro Bayesiano com Spam

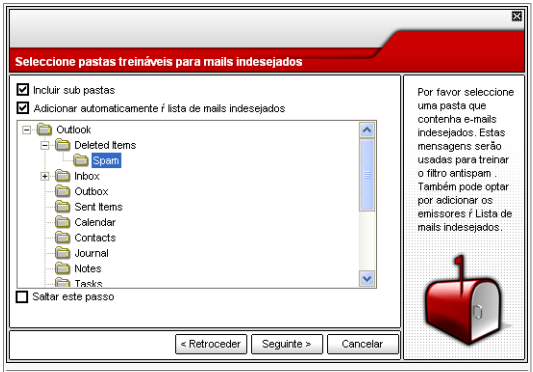

Figura 9.15. Treinar o filtro Bayesiano com Spam

Por favor seleccione a pasta que contém mensagens de e-mail de spam. Estas mensagens serão usadas para treinar o filtro Bayesiano.

Importante

Por favor certifique-se que a pasta que escolher não contém, de modo algum, e-mails legítimos; de outro forma, o desempenho do Antispam será consideravelmente reduzido.

No lado superior da janela estão disponíveis duas opções:

- **Incluir sub-pastas** - para incluir as sub-pastas à sua selecção;
- **Adiconar automaticamente à lista spammers** - para adicionar os remetentes à **Lista de Spammers**.

Seleccione **Saltar este passo** se pretender omitir este passo. Clique em **Retroceder** para voltar ao passo anterior ou clique em **Seguinte** para continuar.

Passo 6/6 - Resumo

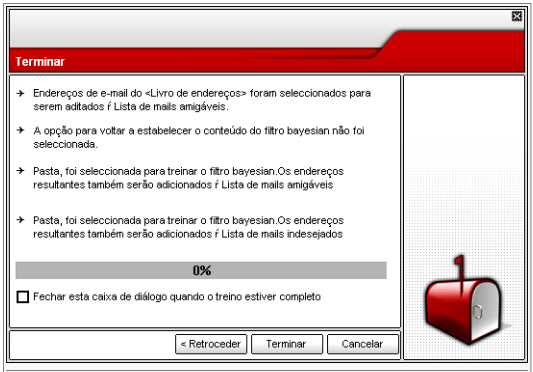
Terminar
Endereços de e-mail do <Livro de endereços> foram seleccionados para serem aditados ŕ Lista de mails amigáveis.
A opção para voltar a estabelecer o conteúdo do filtro bayesian não foi seleccionada.
Pasta, foi seleccionada para treinar o filtro bayesian.Os endereços resultantes também serão adicionados ŕ Lista de mails amigáveis
Pasta, foi seleccionada para treinar o filtro bayesian.Os endereços resultantes também serão adicionados ŕ Lista de mails indesejados
0%
Fechar esta caixa de diálogo quando o treino estiver completo
< Retroceder
Terminar
Cancelar

Figura 9.16. Resumo

Nesta janela pode ver todas as configurações do assistente de configuração. Pode efectuar alterações, retrocedendo aos passos anteriores (clique em **Retroceder**).

Se não deseja fazer quaisquer modificações, clique em **Terminar** para finalizar o assistente.

Capítulo 10. Módulo Antispyware

A secção de **Antispyware** deste guia do utilizador contém os seguintes tópicos:

- Estado do Antispyware
- Configuração Avançada - Controlo de Privacidade
- Configuração Avançada - Controlo de Registo
- Configuração Avançada - Controlo de Ligação
- Configuração Avançada - Controlo de Cookies
- Configuração Avançada - Controlo de Script
- Informação do Sistema

Nota

Para mais detalhes com respeito ao módulo **Antispyware** consulte a descrição do "*Módulo Antispyware*" (p. 32).

10.1. Estado do Antispyware

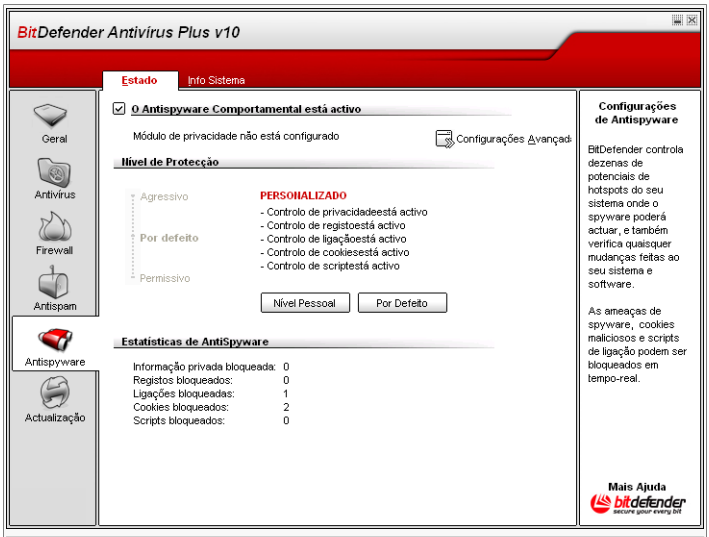

Figura 10.1. Estado do Antispyware

Nesta secção pode configurar o **Antispyware Comportamental** e pode ver informação acerca da sua actividade.

Importante

Para evitar que o spyware infecte o seu computador mantenha o **Antispyware Comportamental** activado.

Ao fundo da secção poderá ver as **Estatísticas do Antispyware**.

O módulo**Antispyware** protege o seu computador contra spywares através de 5 controlos de protecção importantes:

- Controlo de Privacidade - protege os seus dados confidenciais ao filtrar o tráfego HTTP e SMTP de acordo com as regras que criou na secção de Privacidade.
- O Controlo do Registo irá pedir a sua permissão sempre que um programa tentar modificar uma entrada de registo de forma a poder ser executado durante o arranque do Windows.

- Controlo de Ligação - irá pedir a sua permissão sempre que um programa de ligação tentar aceder ao modem do computador.
- O Controlo de Cookies irá pedir a sua permissão sempre que um novo site web tentar definir um cookie.
- O Controlo de script irá pedir a sua permissão sempre que um site web tente activar um script ou outro conteúdo activo.

Para definir as configurações para estes controlos clique em Configuração Avançada.

10.1.1. Nível de Protecção

Pode escolher o nível de protecção que melhor se adapta às suas necessidades de segurança. Arraste o marcador ao longo da escala para definir o nível de segurança apropriado.

Existem 3 níveis de protecção:

Nível de Protecção	Descrição
Permissivo	Apenas o **Controlo de Registo** está activo.
Por Defeito	O **Controlo de Registo** e o **Controlo de Ligação** estão activos.
Agressivo	O **Controlo de Registo**, o **Controlo de Ligação** e o **Controlo de Privacidade** estão activos.

Pode personalizar o nível de protecção ao clicar em **Nível Personalizado**. Na janela que irá aparecer, seleccione os controlos Antispyware que pretende activar e clique em **OK**.

Clique em **Nível por Defeito** para colocar o mostrador no nível por defeito.

10.2. Configuração Avançada - Controlo de Privacidade

Para aceder a esta secção clique no botão **Configuração Avançada** do módulo **Antispyware**, secçãoEstado.

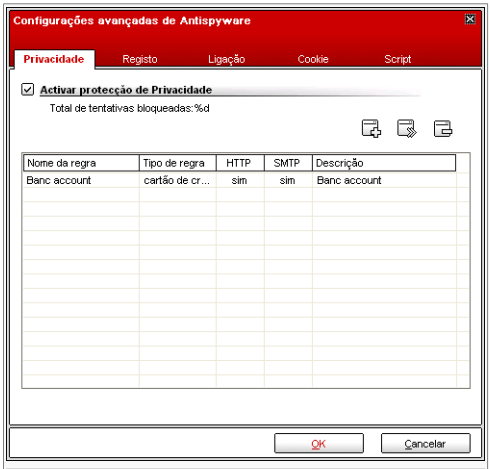

Figura 10.2. Controlo de Privacidade

Manter informação confidencial segura é um assunto importante que nos preocupa a todos. O roubo de dados tem crescido com o desenvolvimento das comunicações Internet e actualmente fazem-se uso de novos métodos para enganar as pessoas e retirar-lhes informação privada.

Quer seja o seu e-mail o seu número de cartão de crédito, quandos eles caem em mãos erradas essa informação poderá causar-lhe danos: poderá encontrar-se afogado em mensagens spam ou poderá ser surpreendido ao aceder à sua conta e verificar que está vazia.

Controlo de Privacidade ajuda-o a manter a sua informação confidencial em segurança. Analisa o tráfego HTTP ou SMTP, ou ambos, para certos caracteres que defeniu. Se for encontrada uma correspondência, a respectiva página web ou e-mail são bloqueados.

As regras podem ser introduzidas manualmente (clique no botão **Adicionar** e escolha os parâmetros da regra). O assistente de configuração irá aparecer.

10.2.1. Assistente de Configuração

O assistente de configuração é um procedimento composto por 3 passos.

Passo 1/3 - Definir Tipo de Regra e Dados

Figura 10.3. Definir Tipo de Regra e Dados

Insira o nome da regra no campo de edição.

Deve definir os seguintes parâmetros:

- **Tipo de Regra** - escolha o tipo de regra (morada, nome, cartão de crédito, PIN, NSS, etc.
- **Dados de Regra** - insira os dados da regra.

Todos os dados que inserir são encriptados. Para uma segurança adicional, não insira todos os dados que deseja proteger.

Clique em **Seguinte**.

Passo 2/3 - Seleccionar Tráfego

Assistente de BitDefender
Passo 2/3
Analisar HTTP
Analisar SMTP
As páginas web que solicitem a sua informação não serão mostradas, e a informação que elas requerem não será enviada. Os e-mails de saída que contenham informação privada serão impedidos de saírem.
< Retroceder
Seguinte >
Cancelar

Figura 10.4. Seleccionar Tráfego

Seleccione o tráfego que quer que o BitDefender analise. As seguintes opções estão disponíveis:

- **Analisar HTTP** - analisa o tráfego HTTP (web) e bloqueia os dados de saída que correspondem aos dados da regra.
- **Analisar SMTP** - analisa todo o tráfego SMTP (mail) e bloqueia as mensagens de e-mail de saída que contém os dados da regra.

Clique em **Seguinte**.

Passo 3/3 – Descrever Regra

Assistente de BitDefender
Passo 3/3
Descrição da regra
Banc account
Insira uma descrição para esta regra. A descrição deverá ajudá-lo a si ou aos outros administradores a identificar facilmente que informação está a ser bloqueada.
< Retroceder
Terminar
Cancelar

Figura 10.5. Descrever Regra

Insira uma breve descrição da regra no campo de edição.

Clique em **Terminar**.

10.2.2. Gerindo as Regras

Pode ver as regras listadas na tabela.

Para apagar uma regra, seleccione-a e clique no botão **Apagar**. Para desactivar temporariamente uma regra sem a apagar, limpe a caixa de selecção correspondente.

Para editar uma regra, seleccione-a e clique no botão **Editar** ou faça duplo-clique sobre ela. Uma nova janela irá aparecer.

Aqui pode mudar o nome, descripção e parâmetros da regra (tipo, dados e tráfego). Clique em **OK** para guardar as alterações.

Figura 10.6. Editar Regra

Clique em **OK** para guardar as alterações e fechar a janela.

10.3. Configuração Avançada - Controlo de registo

Para aceder a esta secção entre na janela **Configuração Avançada de Antispyware** (vá ao módulo de **Antispyware**, secção deEstado e clique em **Configuração Avançada**) e clique no botão **Registo**.

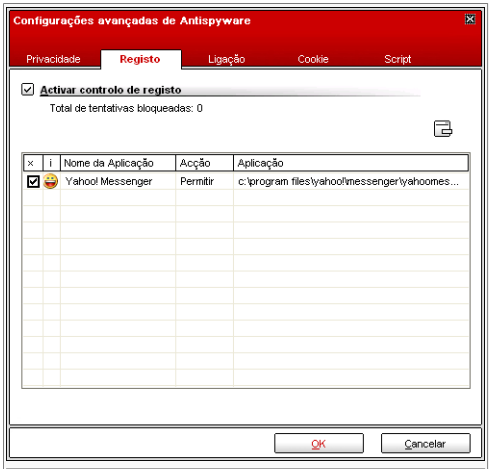

Figura 10.7. Controlo de Registo

Uma parte muito importante do sistema operativo do Windows é chamado de **Registo**. Aqui é o local onde o guarda as suas definições, programas instalados, informação acerca do utilizador e por aí fora.

O **Registo** também é utilizado para definir quais os programas que deverão ser lançados automaticamente ao iniciar o Windows. Frequentemente, os vírus usam isto para se lançarem automaticamente quando o utilizador reiniciar o seu computador.

O **Controlo de registo** vigia o Registo do Windows – mais uma vez, isto é útil para detectar Cavalos de Tróia. Irá alertá-lo sempre que um programa tente modificar uma entrada de registo para poder ser executado ao iniciar o Windows.

Alerta de registo
Yahoo! Messenger
Caminho: c:\program files\yahoo!\messenger\yahoomessenger.exe
Pergunta:
Este programa está a tentar modificar uma entrada do registo.
Isto permitirá que o programa se execute automaticamente ao iniciar o Windows.
Deseja permitir isso?
Recomendação do BitDefender: permitir acesso
Empresa: Yahoo! Inc.
Versão: 8.1.0.195
Copyright: (c) 1998-2006 Yahoo! Inc. All rights reserved.
Memorizar esta resposta
Sim
Não

Figura 10.8. Alerta de registo

Pode negar esta modificação ao clicar em **Não** ou pode permitir ao clicar em **Sim**.

Se deseja que o BitDefender memorize esta resposta tem de seleccionar a caixa de selecção: **Memorizar esta resposta**.

Nota

As suas respostas serão a base deste conjunto de regras.

Para eliminar uma entrada de registo, basta seleccioná-la e clicar no botão **Apagar**. Para desactivar uma entrada de registo temporariamente sem a eliminar, desmarque a caixa de selecção correspondente.

Nota

O BitDefender irá, normalmente, alertá-lo quando instalar novos programas que necessitem de se executar durante o iniciar do seu computador. Na maioria dos casos, estes programas são legítimos e de confiança.

Clique em **OK** para fechar a janela.

10.4. Configuração Avançada - Controlo de Ligação

Para aceder a esta secção entre na janela **Configuração Avançada de Antispyware** (vá ao módulo de **Antispyware**, secção deEstado e clique em **Configuração Avançada**) e clique no botão **Ligação** .

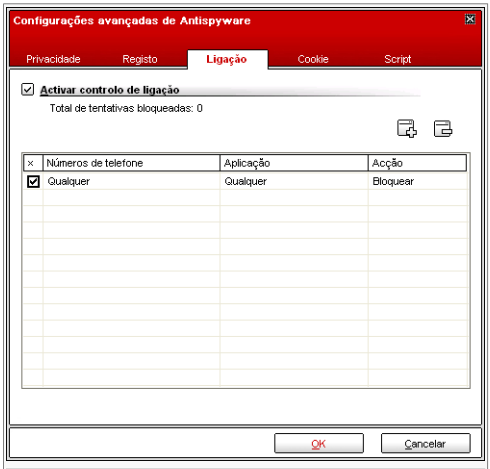

Figura 10.9. Controlo de Ligação

Os dialers são aplicações que usam os modems do computador para marcar diferentes números de telefone. Normalmente, os dialers são utilizados para aceder a vários locais ao marcar números de telefone caros.

Com o **Controlo de Ligação** pode decidir que ligações a diferentes números de telefone, deseja permitir ou bloquear. Esta função controla todos os dialers que tentam aceder ao modem do computador, avisando imediatamente o utilizador e alertando-o para que escolha se pretende bloquear ou permitir tais operações:

Figura 10.10. Alerta de Ligação

Pode ver o nome e o número de telefone da aplicação.

Seleccione **Memorizar esta pergunta** e clique em **Sim** ou **Não** e é criada uma nova regra, a ser aplicada e listada na tabela de regras. Já não será notificado quando a aplicação tentar marcar o mesmo número de telefone.

Toda a regra que foi memorizada pode ser acedida na secção **Ligação** para futura afinação.

Importante

A prioridade das regras é feita de cima para baixo, o que significa que a primeira regra tem a maior prioridade. Faça Drag&drop às regras para alterar a sua prioridade.

Para eliminar uma regra, basta seleccioná-la e clicar no botão **Apagar**. Para modificar o parâmetro de uma regra, basta fazer um duplo-clique no seu campo e fazer a modificação desejada. Para desactivar temporariamente a regra, sem a apagar, desmarque a caixa de selecção correspondente.

As regras podem ser introduzidas automaticamente (através da janela de alerta) ou manualmente (clique no botão **Adicionar** e escolha os parâmetros para a regra). O assistente de configuração irá aparecer.

10.4.1. Assistente de Configuração

O assistente de configuração é um procedimento com 2 passos.

Passo 1/2 - Seleccionar Aplicação e Acção

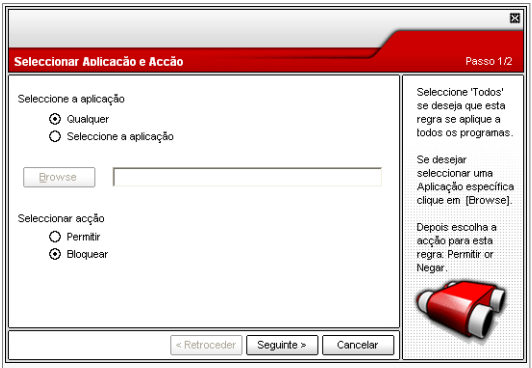

Figura 10.11. Seleccionar Aplicação e Acção

Pode definir os parâmetros:

- **Aplicação** - selecciona a aplicação para a regra. Pode escolher apenas uma aplicação (clique em **Seleccionar aplicação**, em seguida **Explorar** e seleccione a aplicação) ou todas as aplicações (basta clicar em **Todas**).

- **Acção** - selecciona a acção da regra.

Acção	Descrição
Permitir	A acção será permitida.
Bloquear	A acção será negada.

Clique em **Seguinte**.

Passo 2/2 - Seleccionar Números de Telefone

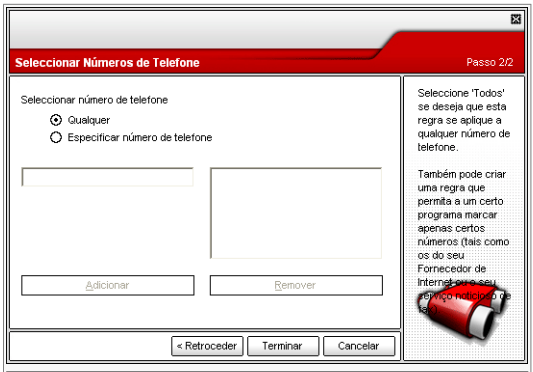
Seleccionar Números de Telefone
Passo 2/2
Seleccionar número de telefone
Qualquer
Especificar número de telefone
Adicionar
Remover
Seleccione 'Todos' se deseja que esta regra se aplique a qualquer número de telefone.
Também pode criar uma regra que permita a um certo programa marcar apenas certos números (tais como os do seu Fornecedor de
« Retroceder
Terminar
Cancelar

Figura 10.12. Seleccionar Números de Telefone

Clique em **Especificar número de telefone**, introduza os números de telefone para os quais criou a regra e clique em **Adicionar**.

Nota

Pode usar wild cards na sua lista de números de telefone a banir; por ex.: 1900* significa que todos os números começados por 1900 serão bloqueados.

Seleccione **Todos** se pretende que esta regra se aplique a qualquer número de telefone. Se deseja eliminar um número, basta seleccioná-lo e clicar em **Remover**.

Nota

Também pode criar uma regra que permita a um programa marcar só certos números (tais como o do seu Serviço de Internet).

Clique em **Terminar**.

Clique em **OK** para guardar as alterações e fechar a janela.

10.5. Configuração Avançada - Controlo de Cookies

Para aceder a esta secção entre na janela **Configuração Avançada de Antispyware** (vá para o módulo**Antispyware**, na secção Estado e clique em **Configuração Avançada**) e clique no botão **Cookie**.

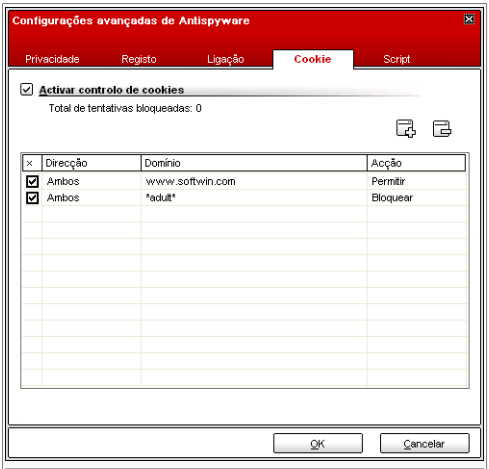

Figura 10.13. Controlo de Cookies

As Cookies são uma ocurrência muito comum na Internet. Elas são ficheiros pequenos armazenados no seu computador. Os sites da Web criam estas cookies para manter um rasto de informação específica sobre si.

As Cookies são geralmente criadas para facilitar a sua vida. Por exemplo, elas podem ajudar o site da Web a lembrar-se do seu nome e preferências, para que não tenha de os voltar a introduzir sempre que os visitar.

Mas as cookies também podem ser usadas para comprometer a sua privacidade, ao seguir o rasto do seu padrão de navegação.

É aqui que o **Controlo de Cookies** ajuda. Quando activo, o **Controlo de Cookies** irá pedir a sua permissão sempre que um site da web tentar estabelecer uma cookie:

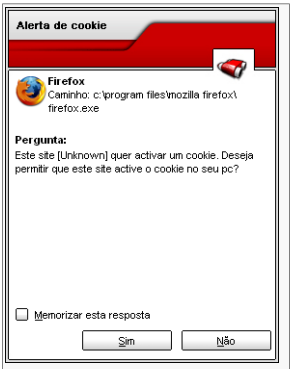
Alerta de cookie
Firefox
Caminho: c:\program files\mozilla firefox\firefox.exe
Pergunta:
Este site [Unknown] quer activar um cookie. Deseja permitir que este site active o cookie no seu pc?
Memorizar esta resposta
Sim
Não

Figura 10.14. Alerta de Cookie

Pode ver o nome da aplicação que está a tentar enviar um ficheiro de cookie.

Seleccione **Memorizar esta pergunta** e clique em **Sim** ou **Não**, e é criada uma nova regra, que é aplicada e listada na tabela de regras. Já não será notificado quando se ligar ao mesmo site.

Isto irá ajudá-lo a escolher quais os sites da web em que pode confiar ou não.

Nota

Devido ao grande número de cookies usadas hoje na Internet, o **Controlo de Cookie** pode ser um pouco aborrecido de início. Inicialmente, irá perguntar uma série de questões acerca de sites que tentam colocar cookies no seu computador. Logo que adicione os seus sites habituais à lista de regras, a navegação tornar-se-á tão fácil como antes.

Toda a regra que foi memorizada pode ser acedida na secção **Cookies** para uma maior afinação.

Importante

A prioridade das regras é feita de cima para baixo, o que significa que a primeira regra tem a maior prioridade. Faça Drag&drop às regras para alterar a sua prioridade.

Para eliminar uma regra, basta seleccioná-la e clicar no botão **Apagar**. Para modificar o parâmetro de uma regra, basta fazer um duplo-clique no seu campo e fazer a modificação desejada. Para desactivar temporariamente a regra, sem a apagar, desmarque a caixa de selecção correspondente.

As regras podem ser introduzidas automaticamente (através da janela de alerta) ou manualmente (clique no botão **Adicionar** e escolha os parâmetros para a regra). O assistente de configuração irá aparecer.

10.5.1. Assistente de Configuração

O assistente de configuração é um procedimento com 1 passo.

Passo 1/1 - Seleccionar Endereço, Acção e Direcção

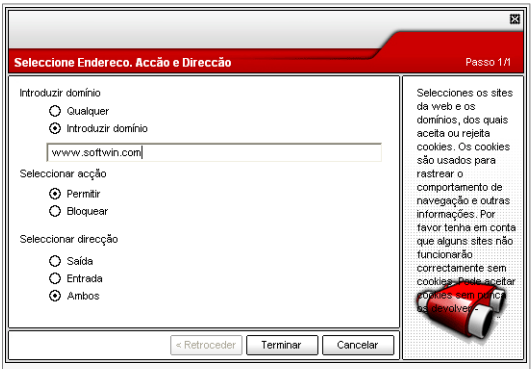
Seleccione Endereco. Acção e Direcção
Passo 1/1
Introduzir domínio
Qualquer
Introduzir domínio
www.softwin.com
Seleccionar acção
Permitir
Bloquear
Seleccionar direcção
Saída
Entrada
Ambos
Selecciones os sites da web e os domínios, dos quais aceita ou rejeita cookies. Os cookies são usados para rastrear o comportamento de navegação e outras informações. Por favor tenha em conta que alguns sites não funcionarão correctamente sem cookies. Pode aceitar cookies sem nunca os devolver.
« Retroceder
Terminar
Cancelar

Figura 10.15. Seleccionar Endereço, Acção e Direcção

Pode definir os parâmetros:

- **Endereço de domínio** - introduza o domínio, ao qual a regra deve aplicar-se.
- **Acção** - selecciona a acção da regra.

Acção	Descrição
Permitir	Os cookies desse domínio serão executados.
Bloquear	Os cookies desse domínio não serão executados.

- **Sentido** - selecciona o sentido do tráfego.

Tipo	Descrição
Saída	A regra será aplicada apenas às cookies que são enviadas para fora para o site a que está ligado.
Entrada	A regra será aplicada apenas às cookies que são recebidas do site a que está ligado.
Ambos	A regra aplica-se em ambos os sentidos.

Clique em **Terminar**.

Nota

Pode aceitar cookies sem nunca as devolver, ao estabelecer a acção para **Negar** e a direcção para **Saída**.

Clique em **OK** para guardar as alterações e fechar a janela.

10.6. Configuração Avançada - Controlo de Script

Para aceder a esta secção entre na janela **Configuração Avançada de Antispyware** (vá ao módulo de **Antispyware**, secção deEstado e clique em **Configuração Avançada**) e clique no botão **Script**

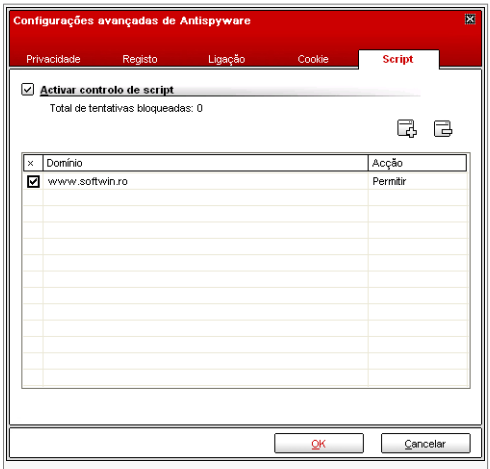

Figura 10.16. Controlo de script

Scripts e outros códigos tais como Controlos de ActiveX e Java applets, os quais são usados para criar páginas da web interactivas, podem ser programados para ter efeitos nocivos. Os elementos do ActiveX, por exemplo, podem ganhar total acesso aos seus dados e podem ler dados do seu computador, informação eliminada, capturar palavras-passe e interceptar mensagens enquanto está ligado. Apenas deverá aceitar conteúdo activo de sites que conhece e confia totalmente.

BitDefender deixa-o escolher entre permitir ou bloquear a execução destes elementos.

Com o **Controlo de script** terá a seu cargo escolher os sites da web, nos quais confia ou não. O BitDefender irá pedir a sua permissão sempre que um site da web tente activar um script ou outro conteúdo activo:

Alerta de script
Firefox
Caminho: c:\program files\mozilla firefox\firefox.exe
Pergunta:
Este programa recebeu conteúdo activo (ActiveX/Java Applet/Script) de [localhost] através do serviço http. Deseja que permitir que este programa o armazene no seu pc?
Memorizar esta resposta
Sim
Não

Figura 10.17. Alerta de Script

Pode ver o nome do recurso.

Seleccione **memorizar esta pergunta** e clique em **Sim** ou **Não**, e é criada uma nova regra, que é aplicada e listada na tabela de regras. Já não será notificado quando o mesmo site tentar enviar-lhe conteúdo activo.

Toda a regra que foi memorizada pode ser acedida na secção **Script** para futura afinação.

Importante

A prioridade das regras é feita de cima para baixo, o que significa que a primeira regra tem a maior prioridade. Faça Drag&drop às regras para alterar a sua prioridade.

Para eliminar uma regra, basta seleccioná-la e clicar no botão **Apagar**. Para modificar o parâmetro de uma regra, basta fazer um duplo-clique no seu campo e fazer a modificação desejada. Para desactivar temporariamente a regra, sem a apagar, desmarque a caixa de selecção correspondente.

As regras podem ser introduzidas automaticamente (através da janela de alerta) ou manualmente (clique no botão **Adicionar** e escolha os parâmetros para a regra). O assistente de configuração irá aparecer.

10.6.1. Assistente de Configuração

O assistente de configuração é um procedimento com 1 passo.

Passo 1/1 - Seleccionar Endereço e Acção

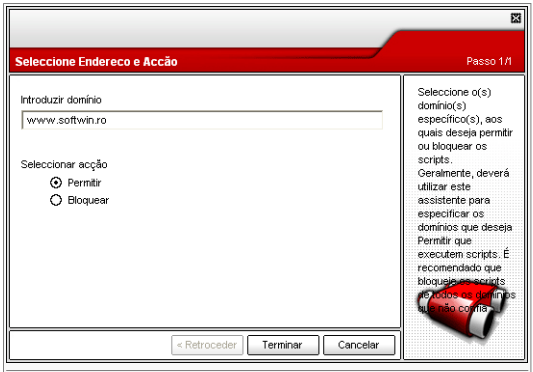
Seleccione Endereco e Accão
Passo 1/1
Introduzir domínio
www.softwin.ro
Seleccionar acção
Permitir
Bloquear
Seleccione o(s) domínio(s) específico(s), aos quais deseja permitir ou bloquear os scripts. Geralmente, deverá utilizar este assistente para especificar os domínios que deseja Permitir que executem scripts. É recomendado que bloqueie os scripts de todos os domínios que não confia.
« Retroceder
Terminar
Cancelar

Figura 10.18. Seleccionar Endereço e Acção

Pode definir os parâmetros:

- **Endereço de domínio** - introduza o domínio, ao qual a regra deve aplicar-se.
- **Acção** - selecciona a acção da regra.

Acção	Descrição
Permitir	Os scripts desse domínio serão executados.
Bloquear	Os scripts desse domínio não serão executados.

Clique em **Terminar**.

Clique em **OK** para guardar as alterações e fechar a janela.

10.7. Info do Sistema

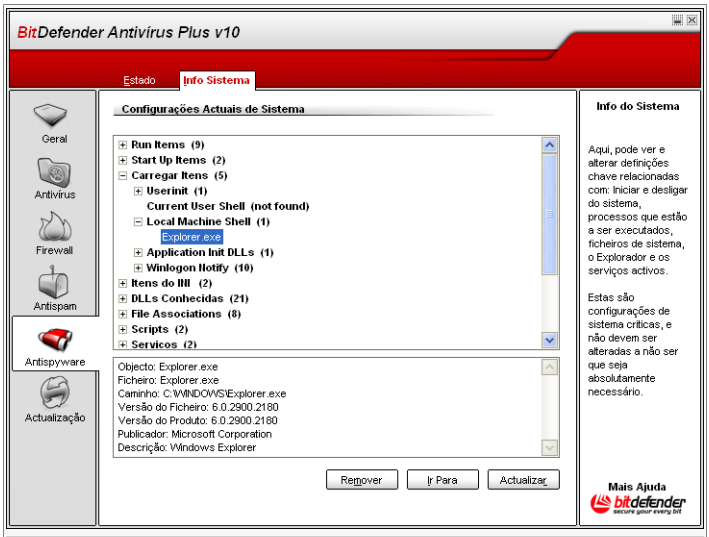

Figura 10.19. Info do Sistema

Aqui pode ver e alterar definições chaves de informação do sistema.

A lista contém todos os itens carregados quando inicia o sistema assim como os itens carregados pelas diferentes aplicações.

Estão disponíveis três botões:

- **Remover** - apaga o item seleccionado.
- **Ir para** - abre uma janela onde o item seleccionado é colocado (o **Registo** por exemplo).
- **Actualizar** - reabre a secção de **Info Sistema**.

Capítulo 11. Módulo de Actualização

A secção de **Actualização** deste guia do utilizador contém os seguintes tópicos:

- Actualização Automática
- Actualização Manual
- Configurações da Actualização

Nota

Para mais detalhes com respeito ao módulo **Actualização** consulte a descrição de "*Módulo de Actualização*" (p. 32).

11.1. Actualização Automática

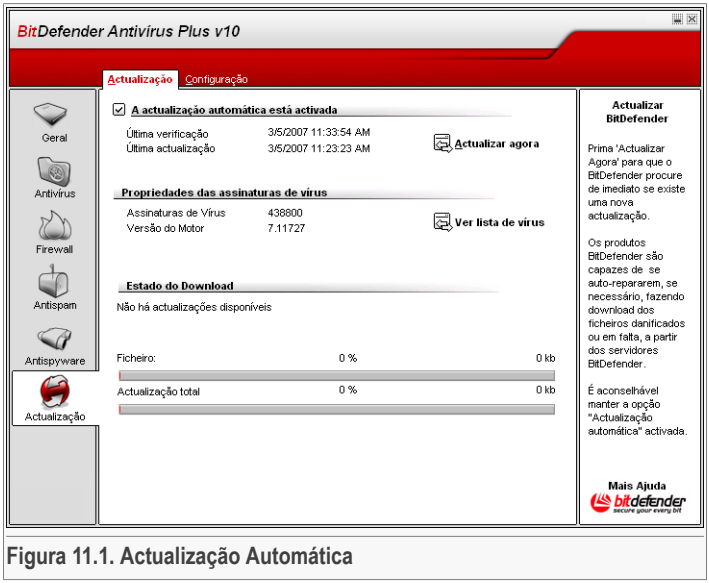
BitDefender Antivírus Plus v10
Actualização
Configuração
Geral
Antivírus
Firewall
Antispam
Antispyware
Actualização
A actualização automática está activada
Última verificação 3/5/2007 11:33:54 AM
Última actualização 3/5/2007 11:23:23 AM
Actualizar agora
Propriedades das assinaturas de vírus
Assinaturas de Vírus 438800
Versão do Motor 7.11727
Ver lista de vírus
Estado do Download
Não há actualizações disponíveis
Ficheiro: 0 % 0 kb
Actualização total 0 % 0 kb
Actualizar BitDefender
Prima 'Actualizar Agora' para que o BitDefender procure de imediato se existe uma nova actualização.
Os produtos BitDefender são capazes de se auto-repararem, se necessário, fazendo download dos ficheiros danificados ou em falta, a partir dos servidores BitDefender.
É aconselhável manter a opção "Actualização automática" activada.
Mais Ajuda
bitdefender

Figura 11.1. Actualização Automática

Nesta secção pode ver a informação relacionada com a actualização e a execução das mesmas.

Importante

Para estar protegido contra as mais recentes ameaças mantenha a **Actualização Automática** activada.

Se está ligado à Internet através de banda larga ou ADSL, o BitDefender executa esta operação sozinho. Quando liga o computador o BitDefender verifica se há novas assinaturas de vírus e depois disso fá-lo a cada **hora** .

Se uma actualização for detectada, dependendo das opções definidas na secção Opções da Actualização Automática, ser-lhe-á solicitada a confirmação para a actualização ou a actualização será feita automaticamente.

A actualização automática pode também ser feita a qualquer altura que deseje clicando no botão **Actualizar Agora**. Esta actualização é também conhecida como **Actualização a pedido do utilizador**.

O módulo de **Actualização** estabelece ligação ao servidor de actualizações do BitDefender e verificará se há actualizações disponíveis. Se detectar uma actualização, dependendo das opções definidas na secção Opções da Actualização Manual, ser-lhe-á solicitada a confirmação para a actualização ou a actualização será feita automaticamente.

Importante

Poderá ser necessário reiniciar o computador quando a actualização tiver terminado. Recomendamos que o faça o quanto antes.

Nota

Se está ligado à Internet através de uma ligação dial-up, então é uma boa ideia adquirir o hábito de actualizar o Bitdefender a seu pedido.

Pode obter as assinaturas de malware do seu BitDefender ao clicar **Mostrar Lista de Vírus**. Um ficheiro HTML que contém todas as assinaturas disponíveis será criado. Clique novamente **Mostrar Lista de Vírus** para ver a lista. Pode procurar uma assinatura específica de malware por entre a base de dados ou clicar **Lista de Vírus BitDefender** para aceder à base de dados de assinaturas BitDefender on-line.

11.2. Actualização Manual

Este método permite instalar as últimas definições de vírus. Para instalar o upgrade da última versão do produto use a Actualização Automática.

Importante

Use a actualização manual quando a actualização automática não pode ser executada ou quando o computador não está ligado à Internet.

Existem 2 formas de executar a actualização manual:

- Com o ficheiro `weekly.exe`;
- Com os `arquivos zip`.

11.2.1. Actualização Manual com o ficheiro `weekly.exe`

O pacote de actualização `weekly.exe` é disponibilizado todas as Sexta-feiras e inclui todas as definições de vírus e upgrades de motor de análise disponíveis até à data.

Para actualizar o BitDefender usando o `weekly.exe`, siga os seguintes passos:

1. Descarregue o weekly.exe e guarde-o localmente no seu disco duro.
2. Localize o ficheiro downloaded e faça duplo-clique nele para executar o assistente de actualização.
3. Clique em **Seguinte**.
4. Seleccione **Aceito os termos da Licença de Acordo** e clique em **Seguinte**.
5. Clique em **Instalar**.
6. Clique em **Terminar**.

11.2.2. Actualização Manual com os `arquivos zip`

Existem dois arquivos zip no servidor de actualizações, que contêm as actualizações dos motores de análise e das assinaturas de vírus: `cumulative.zip` e `daily.zip`.

- `cumulative.zip` é disponibilizado todas as semanas na Segunda-feira e inclui todas as definições de vírus e actualizações dos motores de análise até à data.
- `daily.zip` é disponibilizado todos os dias e inclui todas as definições de vírus e actualizações dos motores da análise desde o último cumulativo e até à data actual.

BitDefender usa uma arquitectura baseada em serviços. Por causa disto o procedimento de substituir as definições de vírus difere de acordo com o sistema operativo:

- Windows NT-SP6, Windows 2000, Windows XP, Windows Vista.
- Windows 98, Windows Millennium.

Windows NT-SP6, Windows 2000, Windows XP, Windows Vista

Siga os seguintes passos:

1. **Descarregue a actualização apropriada.** Se é Segunda-feira, por favor descarregue o cumulative.zip e guarde-o algures no seu disco. De outra forma descarregue o daily.zip e guarde-o no seu disco. Se é a primeira vez que faz a actualização de forma manual, por favor descarregue ambos os ficheiros.
2. **Pare a protecção antivírus BitDefender.**
   - **Saia da consola de administração BitDefender.** Clique-direito no ícone do BitDefender que está na área de notificação e seleccione **Sair**.
   - **Abrir Serviços.** Clique em **Iniciar**, depois **Painel de Controlo**, duplo-clique em **Ferramentas Administrativas** e depois clique em **Serviços**.
   - **Pare o serviço BitDefender Virus Shield.** Seleccione o serviço **BitDefender Virus Shield** a partir da lista e clique em **Parar**.
   - **Pare o Serviço BitDefender Scan Server.** Seleccione o serviço **BitDefender Scan Server** a partir da lista e clique em **Parar**.
3. **Extraia o conteúdo do ficheiro.** Comece com o `cumulative.zip` quando ambos os ficheiros de actualização estão disponíveis. Extraia o conteúdo para a pasta `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` e aceite a sobrescrita dos ficheiros existentes.
4. **Reinicie a protecção antivírus BitDefender.**
   - **Iniciar o serviço BitDefender Scan Server.** Seleccione o serviço **BitDefender Scan Server** da lista e clique em **Iniciar**.
   - **Iniciar o serviço BitDefender Virus Shield.** Seleccione o serviço **BitDefender Virus Shield** da lista e clique em **Iniciar**.
   - **Abra a Consola de administração BitDefender.**

Nota

Se tem o Windows Vista instalado, será solicitado para confirmar a maioria destas acções.

Windows 98, Windows Millennium

Siga os seguintes passos:

1. **Descarregue a actualização apropriada.** Se é Segunda-feira, por favor descarregue o cumulative.zip e guarde-o algures no seu disco. De outra forma descarregue o daily.zip e guarde-o no seu disco. Se é a primeira vez que faz a actualização de forma manual, por favor descarregue ambos os ficheiros.
2. **Extraia o conteúdo do ficheiro.** Comece com o `cumulative.zip` quando ambos os ficheiros de actualização estão disponíveis. Extraia o conteúdo para a pasta

`C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\`
e aceite a sobrescrita dos ficheiros existentes.

3. **Reinicie o computador.**

11.3. Definições de actualização

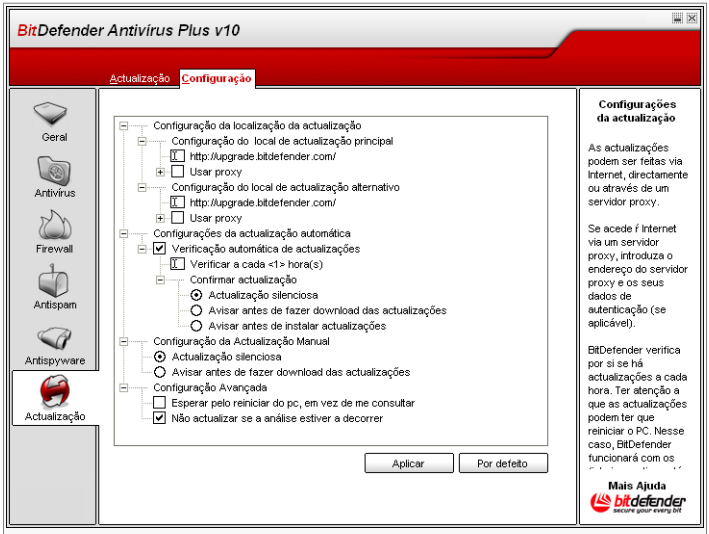
BitDefender Antivírus Plus v10
Actualização
Configuração
Geral
Antivírus
Firewall
Antispam
Antispyware
Actualização
Configuração da localização da actualização
Configuração do local de actualização principal
http://upgrade.bitdefender.com/
Usar proxy
Configuração do local de actualização alternativo
http://upgrade.bitdefender.com/
Usar proxy
Configurações da actualização automática
Verificação automática de actualizações
Verificar a cada <1> hora(s)
Confirmar actualização
Actualização silenciosa
Avisar antes de fazer download das actualizações
Avisar antes de instalar actualizações
Configuração da Actualização Manual
Actualização silenciosa
Avisar antes de fazer download das actualizações
Configuração Avançada
Esperar pelo reiniciar do pc, em vez de me consultar
Não actualizar se a análise estiver a decorrer
Aplicar
Por defeito
Configurações da actualização
As actualizações podem ser feitas via Internet, directamente ou através de um servidor proxy.
Se acede í Internet via um servidor proxy, introduza o endereço do servidor proxy e os seus dados de autenticação (se aplicável).
BitDefender verifica por si se há actualizações a cada hora. Ter atenção a que as actualizações podem ter que reiniciar o PC. Nesse caso, BitDefender funcionará com os
Mais Ajuda
bitdefender

Figura 11.2. Definições de actualização

As actualizações podem ser executadas através da rede local, da Internet, directamente ou através de um servidor proxy.

A janela com as configurações da actualização contém quatro opções de categorias (**Configuração para a actualização**, **Opções de actualização automática**, **Configuração de Actualização Manual** e **Opções Avançadas**) organizadas num menu expandível, semelhante aos do Windows.

Nota

Clique na caixa marcada com o sinal "+" para abrir a categoria ou clique na que está marcada com o sinal "-" para fechar a categoria.

11.3.1. Configuração para a Localização das Actualizações

Para actualizações mais rápidas e fiáveis, pode configurar dois locais de actualização: um **Local primário de actualização** e um **Local alternativo de actualização**. Para ambos deverá configurar as seguintes opções:

- **Local de Actualização** - Se está ligado a uma rede local que tem as assinaturas do BitDefender disponíveis localmente, pode mudar essa localização aqui. Por defeito esta é: http://upgrade.bitdefender.com.
- **Uso do proxy** - No caso da empresa usar um servidor proxy, marque esta opção. Têm de estar especificadas as seguintes definições:
  - **Definições do proxy** - introduza o IP ou o nome do servidor proxy e a porta que o BitDefender utiliza para se conectar ao servidor proxy.

    Importante

    Sintaxe: `nome:porta` ou `ip:porta`.

  - **Utilizador do proxy** - introduza um nome de utilizador reconhecido pelo proxy.

    Importante

    Sintaxe: `dominio\utilizador`.

  - **Palavra-passe do proxy** - introduza uma palavra-passe válida para o utilizador previamente definido.

11.3.2. Opções de Actualização Automática

- **Procura automática de actualizações** - O BitDefender verifica automaticamente os nossos servidores à procura de actualizações disponíveis.
- **Verificar cada x horas** - Estabelece a frequência, na qual o BitDefender verifica se há actualizações. O intervalo, por defeito, é uma hora.
- **Actualização silenciosa** - O BitDefender faz automaticamente o download e a implementação da actualização.
- **Avisar antes de fazer download das actualizações** - cada vez que uma actualização está disponível, será consultado antes do download ser feito.
- **Avisar antes de instalar actualizações** - cada vez que uma actualização for download, será consultado antes da sua instalação ser feita.

Importante

Se seleccionar **Avisar antes de fazer download** ou **Avisar antes de instalar** e fechar&sair da consola de administração a actualização automática não será executada.

11.3.3. Configuração da Actualização Manual

- **Actualização silenciosa** - a actualização manual será feita em background automaticamente.
- **Avisar antes de fazer download das actualizações** - cada vez que leva a cabo uma actualização manual será consultado antes de fazer download e instalar as actualizações.

Importante

Se seleccionar **Avisar antes de fazer download das actualizações** e fizer fechar&sair da consola de administração a actualização manual não será executada.

11.3.4. Opções Avançadas

- **Esperar pelo reiniciar, em vez de o solicitar** - Se uma actualização requer um reiniciar, o produto continuará a funcionar com os antigos ficheiros até que o sistema reinicie. Ao utilizador não lhe será solicitado que o reinicie, logo o processo de actualização do BitDefender não interferirá com o trabalho do utilizador.
- **Não actualizar se a análise estiver a decorrer** - O BitDefender não vai actualizar se estiver a decorrer uma análise. Desta forma, o processo de actualização do BitDefender não vai interferir com as tarefas de análise.

Nota

Se o BitDefender for actualizado enquanto a análise estiver a decorrer, o processo de análise será cancelado.

Clique em **Aplicar** para guardar as alterações, ou clique em **Por Defeito** para retornar às definições por defeito.

Dicas de Utilização

Capítulo 12. Dicas de Utilização

A secção de **Dicas de Utilização** deste manual do utilizador contém os seguintes tópicos:

- Como Proteger o seu Computador Ligado À Internet
- Como Proteger o Seu Computador contra as Ameaças de Malware
- Como Configurar uma tarefa de Análise
- Como Manter o seu Computador Livre do Spam

12.1. Como Proteger o seu Computador Ligado À Internet

Siga estes passos para proteger o seu computador ligado à Internet:

1. **Complete o Assistente Inicial de Instalação .** Durante o processo de instalação um assistente aparecerá. O assistente irá ajudá-lo a registar o seu BitDefender, criar uma conta BitDefender e configurar o BitDefender para executar tarefas de segurança importantes.

   Importante

   Se tem um Cd de Emergência BitDefender Antivirus Plus v10 , analise o seu sistema antes de instalar o BitDefender para limpar qualquer malware que possa existir no seu sistema.

2. **Actualizar o BitDefender.** Se não completou o assistente inicial de instalação, durante o processo de instalação, execute uma actualização a pedido do utilizador (vá para o módulo **Actualização**, secção deActualização, e clique em **Actualizar Agora**).

3. **Executar uma análise completa do sistema.** Aceder ao módulo**Antivírus**, secção Escudo e clique em **Analisar Agora**.

   Nota

   Pode também iniciar uma análise completa ao sistema a partir da secção Analisar. Seleccione a tarefa **Análise Completa do Sistema** e clique em **Executar Tarefa**.

4. **Prevenir a infecção.** Na secção **Escudo** mantenha activa aprotecção em tempo-real de forma a estar protegido contra os vírus, spyware e outro malware.

Defina o nível de protecção que vai de encontro às suas necessidades. Pode personalizar [57] o mesmo sempre que desejar ao clicar em **Nível Personalizado**.

Importante

Programe o seu BitDefender para analisar o seu sistema pelo menos uma vez por semana agendando uma tarefa de **Análise Completa do Sistema** na secçãoAnalisar.

5. **Mantenha o seu BitDefender actualizado.** No módulo da **Actualização**, na secção de Actualização mantenha a opção **Actualização Automática** activa de forma a estar protegido contra as ameaças mais recentes.
6. **Prevenir Ataques da Internet.** Configure a Firewall BitDefender de forma a estar protegido contra ataques da Internet.
7. **Bloquear ferramentas de spyware.** No módulo **Antispyware** ,na secção Estado mantenha a protecção no nível recomendado ou superior. Desta forma, estará protegido contra programas ilegítimos que tentam modificar entradas do registo e contra ligações de elevado custo. Se deseja manter a sua informação confidencial segura active o Controlo de Privacidade e crie as regras apropriadas.
8. **Manter o spam afastado.** Se tem uma conta de e-mail que deseja proteger, configure o módulo Antispam .

12.2. Como Proteger o Seu Computador contra as Ameaças de Malware

Siga estes passos para proteger o seu computador contra os vírus, spyware e outro malware:

1. **Complete o Assistente Inicial de Instalação .** Durante o processo de instalação um assistente aparecerá. O assistente irá ajudá-lo a registar o seu BitDefender, criar uma conta BitDefender e configurar o BitDefender para executar tarefas de segurança importantes.

Importante

Se tem um Cd de Emergência BitDefender, analise o seu sistema antes de instalar o BitDefender para limpar qualquer malware que possa existir no seu sistema.

2. **Actualizar o BitDefender.** Se não completou o assistente inicial de instalação, durante o processo de instalação, execute uma actualização a pedido do utilizador (vá para o módulo **Actualização**, secção deActualização, e clique em **Actualizar Agora**).

3. **Executar uma análise completa do sistema.** Aceder ao módulo**Antivírus**, secção Escudo e clique em **Analisar Agora**.

> **Nota**
> Pode também iniciar uma análise completa ao sistema a partir da secção Analisar. Seleccione a tarefa **Análise Completa do Sistema** e clique em **Executar Tarefa**.

4. **Prevenir a infecção.** Na secção **Escudo** mantenha activa aprotecção em tempo-real de forma a estar protegido contra os vírus, spyware e outro malware. Defina o nível de protecção que vai de encontro às suas necessidades. Pode personalizar [57] o mesmo sempre que desejar ao clicar em **Nível Personalizado**.

> **Importante**
> Programe o seu BitDefender Antivirus Plus v10 para analisar o seu sistema pelo menos uma vez por semana ao agendar uma tarefa de **Análise Completa do Sistema** a partir da secção Analisar.

5. **Mantenha o seu BitDefender actualizado.** No módulo da **Actualização**, na secção de Actualização mantenha a opção **Actualização Automática** activa de forma a estar protegido contra as ameaças mais recentes.
6. **Agendar uma análise completa do sistema.** Vá para a secção**Analisar** e programe o BitDefender para analisar o seu sistema pelo menos uma vez por semana aoagendar usando a tarefa **Análise Completa do Sistema**.

12.3. Como Configurar uma Tarefa de Análise

Siga estes passos para criar e configurar uma tarefa de análise:

1. **Criar uma nova tarefa.** Vá para a secção Analisar e clique em **Nova Tarefa**. A janela das Propriedades irá aparecer.

> **Nota**
> Pode também criar uma nova tarefa ao duplicar uma que já existe. Para fazer isto, faça clique com o botão direito sobre uma tarefa e seleccione **Duplicar** do menu de atalho. Seleccione o duplicado e clique em **Propriedades** para abrir a janela das **Propriedades**.

2. **Definir o nível de análise.** Vá para a secção **Visão Geral** para definir o nível de análise. Se desejar, pode personalizar [65] as configurações da análise ao clicar em **Personalizar**.

3. **Definir o alvo da análise.** Vá para a secção **Analisar Caminho**, e escolha os objectos que quer analisar.
4. **Agendar a tarefa.** Se a tarefa de análise é complexa, poderá ter que a agendar para mais tarde, para uma altura em que o seu computador esteja em descanso. Isto ajudará o BitDefender a executar uma análise mais precisa ao sistema. Vá para a secção do **Agendador** e agende a tarefa.

12.4. Como Manter o seu Computador Livre de Spam

Siga estes passos de forma a manter o Spam afastado do seu computador:

1. **Definir o nível de tolerância.** Aceda ao módulo **Antispam** , e à secção Estado para definir o nível de tolerância. Escolher o nível de tolerância apropriado irá ajudar a que os seus e-mails legítimos cheguem à caixa de Entrada de correio, quer receba quer não uma grande quantidade de e-mails comerciais legítimos ou um elevado volume de spam.
2. **Completar o assistente de configuração de antispam.** Se está a usar o Microsoft Outlook ou o Microsoft Outlook Express / Windows Mail, siga o assistente de configuração que aparece na primeira vez que acede ao seu programa de e-mail. Pode também abrir o assistente a partir da Barra de tarefas Antispam.
3. **Preencher a Lista de Amigos.** Aceda ao módulo **Antispam** , e à secção Estado e clique em ou clique no botão **Amigos** da Barra de tarefas Antispam para abrir a **Lista de Amigos**. Adicione os endereços das pessoas das quais necessita absolutamente os e-mails à Lista de Amigos.

   Nota
   O BitDefender não bloqueia mensagens das pessoas dessa lista; logo, adicionar amigos ajuda a que as mensagens legítimas cheguem a si.

4. **Treinar o Motor de Aprendizagem (bayesiano).** Cada vez que receba um e-mail que considera spam, mas que o BitDefender não o marcou como tal, seleccione-o e clique no botão **É Spam** da barra de tarefas antispam. Futuras mensaqens que tenham o mesmo padrão serão marcadas como SPAM.

   Nota
   O **Motor de Aprendizagem** activa-se apenas após o ter treinado com mais de 60 mensagens de e-mail legitimas. Para fazer isso tem de seguir o assistente de configuração.

5. **Mantenha o seu BitDefender actualizado.** No módulo **Actualização** , na secção Actualização , mantenha a **Actualização Automática** activada de forma a estar protegido contra as novas ameaças à medida que elas surgem.

Nota

Cada vez que executa uma actualização:
- novas assinaturas de imagens serão adicionadas ao **Filtro de Imagem**;
- novos links serão adicionados ao **Filtro de URL**;
- novas regras serão adicionadas ao **filtro NeuNet (Heurístico)**.

Isto ajuda a aumentar a eficácia do motor Antispam.

6. **Configurar o filtro de Caracteres.** A maior parte das mensagens de spam estão escritas comCaracteres cirílicos e / ou asiáticos. Vá ao módulo **Antispam** , à secção Configurações e seleccione **Bloquear Asiático/Bloquear Cirílico** se deseja rejeitar todas as mensagens de e-mail escritas com esses caracteres.

Nota

Pode activar/desactivar cada um destes filtros Antispam na secção Configuração, do módulo**Antispam**.

CD de Emergência BitDefender

BitDefender Antivirus Plus v10 vem num CD de arranque (baseado em LinuxDefender) capaz de analisar e desinfectar todos os discos duros antes de o seu sistema operativo iniciar.

Deve usar o CD de Emergência BitDefender em qualquer altura que o seu sistema operativo não esteja a funcionar bem devido a infecções com vírus. Isso normalmente acontece quando não tem instalado um produto antivírus.

A actualização das assinaturas dos vírus é feita automaticamente, sem haver necessidade de intervenção por parte do utilizador, cada vez que arranca com o Cd de Emergência do BitDefender.

LinuxDefender é uma distribuição do Knoppix recompilada por BitDefender, que integra a mais recente solução BitDefender de segurança para Linux dentro do CD ao Vivo GNU/Linux Knoppix, que lhe oferece uma protecção instantânea de antivirus/antispam de SMTP e um antivírus que é capaz de analisar e desinfectar discos duros existentes (incluindo partições Windows NTFS), partilhas remotas Samba/Windows ou pontos de montagem NFS. Um interface de configuração baseado na web para as soluções BitDefender também está incluido.

Capítulo 13. Geral

Características Importantes

- Protecção instantânea de e-mail (Antivirus & Antispam)
- Soluções antivírus para o seu disco duro
- Suporte de escrita em NTFS (usando Captive project)
- Desinfecção de ficheiros infectados das partições do Windows XP

13.1. O que é o KNOPPIX?

Declaração de http://knopper.net/knoppix:

“ KNOPPIX is a bootable CD with a collection of GNU/Linux (http://www.linux.com/) software, automatic hardware detection, and support for many graphic cards, sound cards, SCSI and USB devices and other peripherals. KNOPPIX can be used as a Linux demo, educational CD, rescue system, or adapted and used as a platform for commercial software product demos. It is not necessary to install anything on a hard disk. ”

13.2. Requisitos do Sistema

Antes de arrancar o LinuxDefender, deve em primeiro lugar verificar se o seu sistema possui os seguintes requisitos.

Tipo de Processador

x86 compatível, mínimo 166 MHz, mas não espere uma boa performance neste caso. A geração i686 de processador, a 800MHz, seria uma escolha mais apropriada.

Memória

O mínimo aceitável são 64MB, o recomendado são 128MB, para uma melhor performance.

CD-ROM

LinuxDefender é executado a partir do CD-ROM, logo um CD-ROM e uma BIOS capaz de arrancar a partir dele são necessários.

ligação Internet

Apesar de LinuxDefender se executar sem ligação à Internet, os processos de actualização requerem uma ligação HTTP activa, mesmo que seja através de

um servidor proxy. Logo, para ter uma protecção actualizada, a Ligação à Internet tem de EXISTIR.

Resolução Gráfica

Uma resolução gráfica mínima de 800x600 é recomendada para a administração baseada na web.

13.3. Software incluído

O CD de Emergência BitDefender inclui os seguintes pacotes de software.

- BitDefender SMTP Proxy (Antispam & Antivirus)
- BitDefender Remote Admin (configuração baseada na web)
- BitDefender Linux Edition (analisador antivírus) + GTK Interface
- Documentação BitDefender (PDF & formato HTML)
- BitDefender Extras (Artwork, Leaflets)
- Linux-Kernel 2.6
- Captive NTFS write project
- LUFS - Linux Userland File System
- Ferramentas para recuperação de dados e reparação de sistemas, mesmo para outros sistemas operativos
- Ferramentas de rede de análise e segurança para administradores de redes
- solução de backup Amanda
- thttpd
- Analisador Ethereal de tráfego de rede, IPTraf IP LAN Monitor
- Nessus network security auditor
- Parted, QTParted and partimage, partition resize, save & recovery solution
- Adobe Acrobat Reader
- Mozilla Firefox Web browser

13.4. BitDefender Linux Security Solutions

O CD LinuxDefender inclui BitDefender SMTP Proxy Antivirus/Antispam para Linux, BitDefender Remote Admin (um interface web para configurar BitDefender SMTP Proxy) e o analisador da Edição BitDefender Antivírus para Linux.

13.4.1. BitDefender SMTP Proxy

O BitDefender para Linux Mail Servers - SMTP Proxy é uma solução de segurança de inspecção de conteúdo, que fornece uma protecção antivírus e antispam ao nível da gateway, ao analisar todo o tráfego de e-mail em busca de malware conhecido e desconhecido. Como resultado de uma tecnologia única, BitDefender para Mail Servers

é compatível com a maioria das plataformas de e-mail existentes e possui o certificado "RedHat Ready".

Esta solução Antivírus e Antispam analisa, desinfecta e filtra tráfego de e-mail para qualquer servidor de e-mail existente, independentemente da plataforma e sistema operativo. O BitDefender SMTP Proxy é iniciado durante o arranque e analisa todo o tráfego de entrada de e-mail. Para configurar BitDefender SMTP Proxy, use BitDefender Remote Admin, seguindo as instruções abaixo.

13.4.2. BitDefender Remote Admin

Pode configurar e administrar os serviços BitDefender remotamente (depois de ter configurado a sua rede) ou localmente, seguindo os passos seguintes:

1. Execute o Firefox browser e carregue o BitDefender Remote Admin URL: https://localhost:8139 (ou faça duplo-clique no ícone BitDefender Remote Admin do seu ambiente de trabalho)
2. Faça log-in com o utilizador "bd" e a palavra-passe "bd"
3. Escolha "SMTP Proxy" no menu da mão direita.
4. Definir o servidor SMTP Real e a porta de listening
5. Adicione os domínios de e-mail para relay
6. Adicione os domínios de rede para relay
7. Escolha "AntiSpam" no menu da esquerda para configurar as capacidades antispam
8. Escolha "AntiVírus" para configurar as acções do BitDefender Antivírus (o que fazer quando um vírus é encontrado, a localização da quarentena)
9. Adicionalmente, pode configurar as "notificações de mail" e as capacidades de registo ("Logger")

13.4.3. BitDefender Linux Edition

O analisador antivírus incluido no LinuxDefender está integrado directamente no ambiente de trabalho. Esta versão apresenta um interface gráfico GTK+.

Apenas explore o seu disco rígido (ou partilhas remotas montadas), clique botão-direito com o rato em qualquer ficheiro ou pasta e seleccione "Analisar com BitDefender". BitDefender Linux Edition irá analisar os itens seleccionados e mostrar um relatório de estado. Para opções mais afinadas consulte a documentação do BitDefender Linux Edition (na pasta de Documentação ou nas páginas do manual do BitDefender) e no programa **/opt/BitDefender/lib/bdc** .

Capítulo 14. LinuxDefender Howto

14.1. Iniciar e Parar

14.1.1. Iniciar LinuxDefender

Para iniciar o CD, prepare a BIOS do seu computador para arrancar pelo CD, coloque o CD na drive e reinicie o computador. Cerifique-se que o seu computador pode arrancar pelo CD.

Espere até ao próximo ecrã aparecer e siga as instruções no ecrã para iniciar o LinuxDefender.

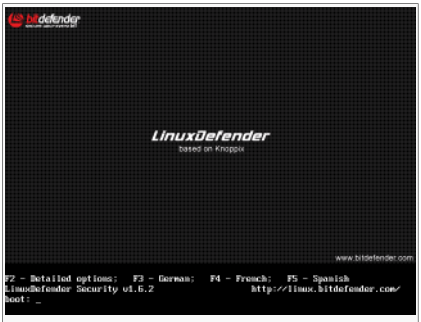

Figura 14.1. Boot Splash Screen

Prima `F2` para opções mais detalhadas. Prima `F3` para opções mais detalhadas em alemão. Prima `F4` para opções mais detalhadas em francês. Prima `F5` para opções mais detalhadas em espanhol. Para um iniciar rápido com as opções por defeito, prima apenas `ENTER`.

Quando o processo de arranque terminar poderá ver o próximo ambiente de trabalho. Pode então começar a usar o LinuxDefender.

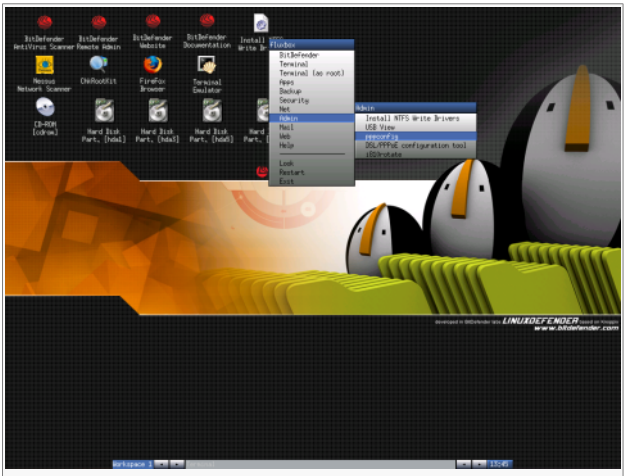

Figura 14.2. O Ambiente de Trabalho

14.1.2. Stop LinuxDefender

Para sair do LinuxDefender de forma apropriada é recomendado que desmonte todas as partições montadas usando o comando**desmontar** ou por clicar botão-direito nos ícones das partições no ambiente de trabalho e seleccionar **Desmontar**. Depois pode desligar em segurança o seu computador ao seleccionar **Sair** a partir do menu LinuxDefender (clique botão-direito para o abrir) ou ao emitir o comando **halt** num terminal.

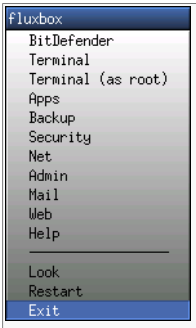

Figura 14.3. Seleccionar "SAIR"

Quando o LinuxDefender fecha com sucesso todos os programas mostra-lhe um ecrã como a imagem seguinte. Pode remover o CD de forma a arrancar pelo seu disco duro. Agora é OK desligar o seu computador ou reiniciá-lo.

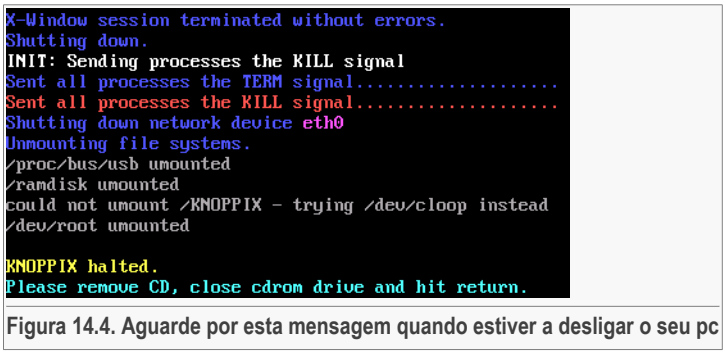
X-Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Sent all processes the TERM signal.....
Sent all processes the KILL signal.....
Shutting down network device eth0
Unmounting file systems.
/proc/bus/usb umounted
/ramdisk umounted
could not umount /KNOPPIX - trying /dev/cloop instead
/dev/root umounted
KNOPPIX halted.
Please remove CD, close cdrom drive and hit return.

Figura 14.4. Aguarde por esta mensagem quando estiver a desligar o seu pc

14.2. Configurar a Ligação à Internet

Se está numa rede DHCP e possui uma placa de rede ethernet, a ligação à Internet deve ser detectada e configurada. Para uma configuração manual, siga os seguintes passos.

1. Abra o menu LinuxDefender (clique-botão direito) e seleccione **Terminal** para abrir a consola.
2. Insira **netcardconfig** no terminal aberto para executar a ferramenta de configuração da rede.
3. Se a sua rede está a usar DHCP, seleccione **sim** (se não tem a certeza, pergunte ao seu administrador de rede). De outra forma, veja em baixo.
4. A configuração de rede deve ser agora automaticamente configurada. Pode ver o seu IP e as configurações da placa de rede com o comando **ifconfig** .
5. Se possui um IP estático (não está a usar DHCP), escolha **Não** na pergunta do DHCP.
6. Siga as instruções no ecrã. Se não tem a certeza do que escrever, contacte o seu administrador de sistema para mais detalhes.

Se tudo está a correr bem, pode testar a sua ligação à Internet ao fazer um "ping" a `bitdefender.com`.

```
$ ping -c 3 bitdefender.com
```

Se está a usar uma ligação dial-up, escolha **pppconfig** a partir do menu Admin / LinuxDefender. Depois siga a instrução no ecrã para definir uma ligação à Internet PPP.

14.3. Actualização BitDefender

Os pacotes BitDefender para o LinuxDefender estão a usar o sistema ramdisk para actualização de ficheiros. Desta forma, pode actualizar todas as assinaturas de vírus, motores de análise ou bases de dados de antispam, mesmo que esteja a executar o sistema a partir de um CD de leitura, como o CD LinuxDefender.

Certifique-se que tem uma ligação à Internet funcional. Primeiro abra o BitDefender Remote Admin e seleccione **Live! Update** do menu à esquerda. Prima **Actualizar Agora** para ver se há actualizações.

Alternadamente, pode inserir o próximo comando num terminal.

```
# /opt/BitDefender/bin/bd  update
```

Todos os processos de actualização são registados no relatório BitDefender por defeito. Pode vê-lo com o próximo comando.

```
# tail  -f /ramdisk/BitDefender/var/log/bd.log
```

Se está a usar um proxy para ligações de saída, configure as definições do Proxy no menu, **Live! Update**, botão**Configuração**.

14.4. Análise de Vírus

14.4.1. Como posso aceder aos meus dados no Windows?

NTFS Write Support

O suporte de escrita NTFS está disponível usando o Captive NTFS write project. Necessita de dois ficheiros drivers da sua instalação do Windows: `ntoskrnl.exe` e `ntfs.sys`. Actualmente, só os drivers do Windows XP são suportados. Tenha em atenção que os pode utilizar para aceder também a partições do Windows 2000/NT/2003.

Instalar os Drivers NTFS

Para aceder às suas partições NTFS do Windows e ser capaz de escrever informação nelas, tem de instalar em primeiro lugar os drivers NTFS. Se não está a usar NTFS nas suas partições Windows, mas FAT, ou se apenas necessita de acesso de leitura

aos seus dados, pode montar directamente as drives e aceder às drives Windows como às drives Linux.

Para adicionar suporte às partições NTFS, tem de instalar primeiro os drivers NTFS, a partir dos seus disco duros, partilhas remotas, sticks USB ou a partir do Windows Update. É recomendado que use os drivers provenientes de uma localização segura porque os drivers locais do Windows podem estar infectados ou corrompidos.

Duplo-clique no ícone **Install NTFS Write Drivers** do ambiente de trabalho para executar o **BitDefender Captive NTFS Installer**. Seleccione a primeira opção se deseja instalar os drivers a partir do disco duro local.

Se os drivers estão numa localização comum, use **Pesquisa Rápida** para encontrar os drivers.

Alternadamente, pode indicar onde se encontram os seus drivers. Ou pode fazer download dos drivers a partir de Windows Update SP1.

Os drivers não são instalados no disco duro, mas são usados temporariamente por LinuxDefender para aceder às partições NTFS do Windows. Se o programa instala os drivers NTFS, pode fazer duplo-clique nos ícones das partições NTFS no ambiente de trabalho e explorar o seu conteúdo. Para explorar os ficheiros com eficiência use o Midnight Commander do menu LinuxDefender (ou insira o comando **mc** na consola).

14.4.2. Como posso levar a cabo uma análise completa ao sistema?

Explore as suas pastas, clique botão-direito num ficheiro ou directoria e seleccione **Enviar para**. Depois escolha **Analisador BitDefender**.

Ou pode emitir o próximo comando de raiz, de um terminal. O **Analisador Antivírus BitDefender** começará com o ficheiro ou pasta seleccionado como a localização por defeito a analisar.

```
# /opt/BitDefender/bin/bdgtk2 /path/to/scan/
```

Depois clique em **Iniciar Análise**.

Se deseja configurar as opções do antivírus, seleccione o botão **Configurar Antivírus** do lado direito do painél do programa.

14.5. Construir um Instant Mail Filtering Toaster

Pode usar o LinuxDefender para criar uma solução de filtragem de mail ad-hoc, sem instalar qualquer software ou modificar o servidor de mail. A ideia por detrás disto é colocar um sistema LinuxDefender à frente do seu servidor de mail, que permita que BitDefender analise em busca de spam e vírus no seu tráfego SMTP e faça relay do mesmo para o verdadeiro servidor de mail.

14.5.1. Pré-requisitos

Necessita de um PC com um CPU Pentium 3 ou compatível ou superior, com pelo menos 256MB de RAM e uma drive de CD/DVD por onde arrancar. O sistema LinuxDefender tem de receber o tráfego SMTP em vez do verdadeiro servidor de mail. Existem diversas formas de fazer esta instalação.

1. Mude o IP do seu verdadeiro servidor de mail e atribua o antigo IP ao sistema LinuxDefender.
2. Modifique os seus registos DNS de forma a que a entrada MX para o seu domínio esteja a apontar para o sistema LinuxDefender.
3. Instale os seus clientes de e-mail para usar o novo sistema LinuxDefender como servidor SMTP.
4. Modifique as suas configurações da firewall para forward / redirect todas as ligações SMTP para o sistema LinuxDefender em vez do verdadeiro servidor de e-mail.

LinuxDefender howto não lhe irá explicar qualquer uma das questões acima. Para mais informação consulte Manuais de Rede Linux e Documentação Netfilter.

14.5.2. O e-mail toaster

Arranque o seu CD LinuxDefender e espere até que o sistema Windows X esteja carregado e funcional.

Para configurar BitDefender SMTP Proxy, faça duplo-clique no ícone **BitDefender Remote Admin** no ambiente de trabalho. A seguinte janela irá aparecer. Use o utilizador`bd` e a palavra-passe`bd` para fazer login no BitDefender Remote Admin.

Após um login bem-sucedido, será capaz de configurar o BitDefender SMTP Proxy.

Escolha **SMTP Proxy** para configurar o verdadeiro servidor de mail que deseja proteger contra o spam e os vírus.

Seleccione o botão **Email domains** para introduzir todos os domínios de e-mail dos quais deseja aceitar e-mails.

Prima **Add Email Domain** ou **Add Bulk Domains** e siga as instruções no ecrã para definir os domínios de relay de e-mail.

Seleccione o botão **Net domains** para inserir todas as redes para as quais deseja fazer relay de e-mail.

Prima **Add Net Domain** ou **Add Bulk Net Domains** e siga as instruções no ecrã para definir os domínios de rede de relay.

Seleccione **Antivirus** do menu da esquerda, para escolhar o que fazer quando um vírus é encontrado e configurar outras opções do antivírus.

Agora, todo o tráfego SMTP é analisado e filtrado por BitDefender. Por defeito, todas as mensagens com vírus são limpas ou bloqueadas e todas as mensagens de spam detectadas por BitDefender são marcadas no Assunto com a palavra `[SPAM]`. Um cabeçalho de e-mail (`X-BitDefender-Spam: Sim/Não`) é adicionado a todos os e-mails para facilitar a filtragem por parte do cliente.

14.6. Perform a Network Security Audit

Beside its anti-malware, data recovery and mail filtering capabilities, LinuxDefender comes with a set of tools that perform an in-depth host & network security audit. Forensics analysis of compromised systems is also possible using the security tools included into LinuxDefender. Read this small tutorial to learn how you can start a quick security audit of your hosts or networks.

14.6.1. Analisar em busca de Rootkits

Before start looking for security issues on networked computers, first be sure that the LinuxDefender host is not compromised. You can perform a virus scanning of installed hard-drives, as shown in **Scan for viruses** tutorial or you can scan for Unix rootkits.

First, mount all your hard-disk partition, double-clicking their desktop icons or by using **mount** command in the console. Then double click the **ChkRootKit** icon to check the CD content or launch the **chkrootkit** command in the console, using `-r NEWROOT` parameter to specify the new / (root) directory of the host.

```
# chkrootkit  -r  /dev/hda3
```

Se um rootkit é encontrado, chkrootkit mostrará o que encontrou em **BOLD**, e usando letras maiúsculas.

14.6.2. Nessus - the Network Scanner

> Nessus is the world's most popular open-source vulnerability scanner used in over 75,000 organizations world-wide. Many of the world's largest organizations are obtaining significant cost savings by using Nessus to audit business-critical enterprise devices and applications.
>
> —*www.nessus.org*

Nessus can be used to remotely scan your network computers against various vulnerabilities. It also recommends some measures to take to mitigate security risks and to prevent security incidents.

Double-click the **Nessus Security Scanner** desktop icon or run **startnessus** from a terminal. Wait until the following window is shown. Depending on your hardware resources, it may take up to 10 minutes for Nessus to load, along its more than 5000 plugins containing vulnerability databases. Use `knoppix` user and `knoppix` password to log in.

Click the **Target selection** tab and enter the computer IP or hostnames you want to scan for vulnerabilities. Make sure you customize all scan options according to your nework or system configuration before you start the scan in order to save tons of bandwidth and resources and have a more accurate scan result. Then click **Start the scan**.

When the scan process is complete, Nessus displays the findings and the recommendations. You can save the report in several formats, including HTML with pies and charts. The saved report can be viewed in your favorite browser.

14.7. Verifique o Estado da RAM do Seu Sistema

Usually, when your system has an unexpected behavior (it hangs or it resets itself from time to time), it may be a memory problem. You can test your RAM modules with the **memtest** program, as described below.

Start your computer and boot from LinuxDefender CD. Type **memtest** at boot-time and press Enter.

The Memtest program will start immediately and it will run several tests to check the RAM status. You can configure what tests to run and other Memtest options, by pressing `c`.

A full Memtest run may take up to 8 hours, depending on your systems RAM capacity and speed. It's recommended to let Memtest run all its tests to entirely check for RAM errors. You can quit at any time, by pressing `ESC`.

If you intend to buy new hardware (a complete system or only some components) it's recommended to use LinuxDefender and memtest to check it for errors or compatibility issues.

Obter Ajuda

Capítulo 15. Suporte

15.1. Departamento de Suporte

Como um fornecedor importante, a SOFTWIN esforça-se por fornecer aos seus clientes um nível de suporte técnico sem igual de uma forma rápida e precisa. O Centro de Suporte (o qual poderá contactar nos endereços que lhe fornecemos abaixo) é continuamente mantido a par das mais recentes ameaças, e é aqui onde todas as suas questões são respondidas de uma forma rápida.

Com o BitDefender, tem sido sempre a nossa prioridade poupar aos nossos clientes tempo e dinheiro ao fornecer-lhes os produtos mais avançados aos preços mais económicos. Mais ainda, pensamos que um negócio de sucesso é baseado numa boa comunicação e num compromisso de excelência no suporte ao cliente.

Convidamo-lo desde já a colocar as suas questões em <bitdefender@realsoft.pt> a qualquer altura. Para uma resposta rápida, por favor inclua no seu e-mail o máximo de detalhes que consiga acerca do seu BitDefender, acerca do seu sistema e uma descrição do problema tão completa e fiel quanto possível.

15.2. Ajuda On-line

15.2.1. BitDefender Knowledge Base

A BitDefender Knowledge Base é um repositório de informação on-line acerca dos produtos BitDefender. Armazena, num formato de relatório facilmente acessível, os resultados das actividades de reparação de erros por parte da equipe técnica do suporte BitDefender e da equipe de desenvolvimento, isto juntamente com artigos gerais acerca de prevenção de vírus, a administração de soluções BitDefender e explicações pormenorizadas, e muitos outros artigos.

A BitDefender Knowledge Base encontra-se aberta ao público e pode ser utilizada gratuitamente. Esta abundância de informação é uma outra forma de dar aos clientes BitDefender o conhecimento e o aprofundamento que eles necessitam. Todos os pedidos de informação ou relatórios de erro válidos originários de clientes BitDefender são incluídos na BitDefender Knowledge Base, como relatórios de reparação de erros, ou artigos informativos como suplementos aos ficheiros de ajuda dos produtos.

A BitDefender Knowledge Base encontra-se disponível a qualquer altura em http://kb.bitdefender.com.

15.3. Informação de Contacto

Comunicação eficiente é a chave de um negócio bem-sucedido. Durante os últimos 10 anos a SOFTWIN estabeleceu uma reputação indiscutível ao exceder as expectativas dos clientes e parceiros, ao procurar constantemente melhorar a comunicação. Por favor não hesite em contactar-nos acerca de qualquer questão ou assunto que nos queira colocar.

15.3.1. Endereços Web

Departmento Comercial: <sales@bitdefender.com>
Suporte Técnico: <support@bitdefender.com>
Documentação: <documentation@bitdefender.com>
Partner Program: <partners@bitdefender.com>
Marketing: <marketing@bitdefender.com>
Contactos Imprensa: <pr@bitdefender.com>
Oportunidades de Trabalho: <jobs@bitdefender.com>
Submeter Vírus: <virus_submission@bitdefender.com>
Submeter Spam: <spam_submission@bitdefender.com>
Relatórios de Abusos: <abuse@bitdefender.com>
Site internacional do produto: http://www.bitdefender.com
Ficheiros ftp do produto: ftp://ftp.bitdefender.com/pub
Distribuidor Local: http://www.bitdefender.com/partner_list
BitDefender Knowledge Base: http://kb.bitdefender.com

15.3.2. Escritórios

Os escritórios BitDefender estão preparados para responder a quaisquer perguntas respeitantes às suas áreas de operação, quer sejam questões comerciais e de assuntos gerais. Os seus respectivos endereços e contactos estão listados abaixo.

Alemanha

Softwin GmbH
Headquarter Western Europe
Karlsdorferstrasse 56
88069 Tettnang
Alemanha
Tel: +49 7542 9444 44
Fax: +49 7542 9444 99
Email: <info@bitdefender.com>

Sales: <sales@bitdefender.com>
Web: http://www.bitdefender.com
Suporte Técnico: <support@bitdefender.com>

UK e Irlanda

One Victoria Square
Birmingham
B1 1BD
Tel: +44 207 153 9959
Fax: +44 845 130 5069
Email: <info@bitdefender.com>
Sales: <sales@bitdefender.com>
Web: http://www.bitdefender.co.uk
Suporte Técnico: <support@bitdefender.com>

Espanha

Constelación Negocial, S.L
C/ Balmes 195, 2a planta, 08006
Barcelona
Soporte técnico: <soporte@bitdefender-es.com>
Ventas: <comercial@bitdefender-es.com>
Phone: +34 932189615
Fax: +34 932179128
Sitio web del producto: http://www.bitdefender-es.com

U.S.A

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Suporte Técnico: <support@bitdefender.com>
Customer Service: 954-776-6262
Web: http://www.bitdefender.com

Romania

SOFTWIN
5th Fabrica de Glucoza St.
PO BOX 52-93
Bucharest
Technical support: <suport@bitdefender.ro>

Sales: <sales@bitdefender.ro>
Phone: +40 21 2330780
Fax: +40 21 2330763
Product web site: http://www.bitdefender.ro

Glossário

ActiveX

O ActiveX é um modelo para fazer programas de forma a que outros programas e o sistema operativo os possam chamar. A tecnologia do ActiveX é usada com o Microsoft Internet Explorer para criar páginas da Web interactivas, que parecem e comportam-se como programas de computador, em vez de páginas estáticas. Com o ActiveX, os utilizadores podem efectuar perguntas ou responder a questões, usando botões para carregar, e interagir de outras formas com a página da Web. Os controlos do ActiveX são frequentemente escritos utilizando o Visual Basic.

O Active X é notável por uma falta completa de controlos de segurança; os especialistas de segurança dos computadores desencorajam o seu uso na Internet.

Adware

O adware é com frequência combinado com uma aplicação hospedeira que é fornecida sem custo desde que o utilizador concorde em aceitar o adware. Por causa das aplicações adware serem normalmente instaladas após o utilizador concordar com uma licença de uso que define o propósito da aplicação, nenhuma ilegalidade é na verdade cometida.

No entanto, anúncios tipo pop-up podem tornar-se bastante incomodativos, e em alguns casos podem mesmo degradar a performance do sistema. Também, a informação que algumas dessas aplicações recolhem podem causar algumas preocupações de privacidade aos utilizadores que não estão completamente conscientes dos termos da licença de uso.

Arquivo

Um disco, cassete, ou directório que contém ficheiros que foram armazenados.

Um ficheiro que contém um ou mais ficheiros num formato comprimido.

Backdoor

Um buraco na segurança de um sistema deliberadamente criado pelos desenhadores ou responsáveis da manutenção. A motivação para tais buracos não é sempre sinistra; alguns sistemas operativos, por exemplo, que trazem contas privilegiadas, criadas para serem usadas pelos técnicos de serviço ou pelo vendedor dos programas de manutenção.

Sector de arranque

Um sector no início de cada disco que identifica a arquitectura do disco (tamanho do sector, tamanho do grupo, e por aí fora). Para discos de inicialização, o sector de saída também contém um programa que carrega o sistema operativo.

Vírus de boot

Um vírus que infecta o sector boot de um disco fixo ou de uma unidade de disquetes. A tentativa de arrancar por uma disquete infectada por um vírus de boot, irá causar a activação do vírus em memória. Sempre que iniciar o seu sistema daquele ponto, terá o vírus activo em memória.

Browser

É um software de aplicação usado para localizar e mostrar páginas da Web. Os dois mais populares motores de busca são o Netscape Navigator e o Microsoft Internet Explorer. Ambos são motores de busca gráficos, o que significa que eles tanto podem mostrar gráficos como texto. Em adição, a maioria dos motores de busca modernos podem apresentar informação multimédia, incluíndo som e vídeo, apesar de requirirem alguns formatos de plug-in.

Linha de comando

Numa interface de linha do comado, o utilizador introduz comandos no espaço providenciado directamente no ecrã, usando a linguagem de comando.

Cookie

Dentro da indústria da Internet, as cookies são descritas como pequenos ficheiros, que contêm informação acerca de computadores individuais, que podem ser analizados e usados pelos publicitários para seguir o rasto online do seus interesses e gostos. Neste domínio, a tecnologia das cookies ainda está a ser desenvolvida e a sua intenção é procurar atingi-lo com publicidade naquilo que disse serem os seus interesses. É uma espada de dois gumes para muitas pessoas, porque, por um lado é eficiente e pertinente já que apenas vê anúncios do seu interesse. Por outro lado, envolve realmente "seguir o rasto" e "perseguir" onde vai e no que clica. Compreensivelmente, existe um debate acerca da privacidade e muitas pessoas sentem-se ofendidas ao terem a noção que estão a ser vistas como um "número SKU " (sabe, o código de barras por detrás das embalagens que é verificado na mercearia). Enquanto este ponto de vista possa ser extremo, em alguns casos é exacto.

drive de disco

É uma máquina que lê os dados do disco e escreve dados num disco.

Uma drive de disco rígido lê e escreve nos discos rígidos.

Uma drive de disquetes acede às disquetes.

As drives dos discos tanto podem ser internas (dentro do computador) ou externas (vêm numa caixa em separado que se liga ao computador).

Download (Descarga)

Para copiar dados (normalmente um ficheiro interno) de uma fonte principal para um aparelho periférico. O termo é frequentemente utilizado para descrever o processo de copiar um ficheiro de um serviço online para o seu próprio computador. Também se pode referir à cópia de um ficheiro de um servidor de ficheiros de rede, para um computador na rede.

E-mail

Correio electrónico. É um serviço que envia mensagens em computadores via redes locais ou globais.

Eventos

Uma acção ou ocorrência detectada por um programa. Os eventos podem ser acções do utilizador, tais como clicar no botão do rato ou carregar numa tecla, ou ocorrências do sistema, tal como ficar sem memória.

Falso positivo

Ocorre quando o analisador identifica um ficheiro como infectado, quando na verdade ele não está.

Extensão do nome do ficheiro

A porção de um nome de ficheiro, que segue o ponto final, a qual indica o tipo de dados armazenados no ficheiro.

Muitos sistemas operativos usam extensões do nome do ficheiro, por ex. Unix, VMS, e MS-DOS. Elas são normalmente de uma a três letras. Os exemplos íncluem ".c" para C de código da fonte, ".ps" para PostEscrito, ".txt" para texto arbitrário.

Heurístico

Um método baseado na regra de identificar novos vírus. Este método de análise que não se baseia em assinaturas específicas de vírus. A vantagem da análise heurística, é que não se deixa enganar por uma nova variante de um vírus existente. Contudo, pode reportar ocasionalmente códigos suspeitos em programas normais, gerando o chamado "falso positivo".

IP

Internet Protocol - Um rótulo de protocolo no protocolo TCP/IP que é responsável dos endereços de IP, rotas, e a fragmentação e reassemblagem dos pacotes de IP.

Java applet

Um programa em Java desenhado para funcionar apenas numa página web. Para usar uma applet numa página web, deverá especificar o nome da applet e

o tamanho (comprimento e largura - em pixels) que a applet pode utilizar. Quando a página da web é acedida, o motor de busca descarrega a applet de um servidor e corre-a apenas na máquina do utilizador (o cliente). As applets diferem das aplicações, pois são administradas por um protocolo de segurança restrito.

Por exemplo, apesar de as applets correrem no cliente, elas não podem escrever nem ler dados na máquina do cliente. Adicionalmente, as applets são restritas para que possam apenas ler e escrever dados provenientes do mesmo domínio do qual elas são servidas.

Macro vírus

Um tipo de vírus de computador que está codificado como uma macro retido num documento. Muitas aplicações, tais como Microsoft Word e Excel, contêm poderosas linguagens macro.

Estas aplicações permitem-lhe reter uma macro num documento, e ter a macro pronta a ser executada sempre que o documento for aberto.

Cliente de mail

Um cliente de e-mail é uma aplicação que lhe permite enviar e receber e-mail.

Memória

Áreas internas de armazenamento no computador. O termo memória identifica armazenamento de dados que vêm na forma de chips, e a palavra armazenar é usada para a memória que existe em cassetes ou discos. Todo o computador vem com uma certa quantidade de memória física, normalmente referida como memória principal ou RAM.

Não-heurístico

Este método de análise depende da assinaturas de vírus especificas. A vantagem de uma análise não-heurística, é que ela não será induzido em erro pelo que possa parecer um vírus e não gera falsos alarmes.

Programas compactados

Um ficheiro num formato compactado. Muitos sistemas operativos e aplicações contêm comandos que lhe permitem compactar um ficheiro, para que ocupe menos memória. Por exemplo, suponha que tem um ficheiro de texto contendo dez espaços de caracteres consecutivos. Normalmente isto iria requerer dez de armazenamento.

Contudo, um programa que compacta ficheiros iria substituir o espaço dos caracteres por uma série-de-espaços de caracteres especial, seguida pelo número de espaços a serem substituidos. Neste caso, os dez espaços iriam requerer apenas dois bytes. Esta é apenas uma técnica de compactar, há muitas.

Caminho

As direcções exactas para um ficheiro num computador. Estas direcções são normalmente descritas por meios de preenchimento hierárquico do topo para baixo.

A rota entre dois quaisquer pontos, tal como os canais de comunicação entre dois computadores.

Phishing

O acto de enviar um e-mail a um utilizador como sendo falsamente uma empresa legítima e estabelecida numa tentativa de levar o utilizador a providenciar informação privada que será utilizada para roubo. O e-mail leva o utilizador a visitar um site na Internet onde lhe é solicitado que actualize informação pessoal, tal como palavras-passe e números de cartões de crédito, segurança social, e números de contas bancárias, que a legítima organização já possui. O site web, no entanto, é falso e está feito apenas para roubar a informação ao utilizador.

Vírus polimórfico

Um vírus que altera a sua forma com cada ficheiro que infecta. Dado que eles não têm uma padrão de patente binária consistente, tais vírus são difíceis de identificar.

Porta

Uma interface num computador, à qual se liga um aparelho. Os computadores pessoais têm vários tipos de portas. Internamente, existem várias portas para ligar componentes de disco, ecrãs, e teclados. Externamente, os computadores pessoais têm portas para ligar modems, impressoars, ratos, e outros aparelhos periféricos.

Nas redes TCP/IP e UDP, um ponto final para uma ligação lógica. O número da porta identifica o tipo da porta. Por exemplo, a porta 80 é usada para o tráfego HTTP.

Ficheiro de relatório

Um ficheiro que lista acções que tiveram ocurrência. O BitDefender mantém um ficheiro de relatório que lista o caminho analisado, as pastas, o número de arquivos e ficheiros examinados, e quantos ficheiros suspeitos e infectados foram encontrados.

Rootkit

Um rootkit é um pacote de ferramentas de software que proporcionam um nível de acesso de administrador a um sistema. O termo foi usado em primeiro lugar nos sistemas operativos UNIX e referia-se a ferramentas recompiladas que proporcionavam aos intrusos direitos de administração, permitindo-lhes ocultar a sua presença de forma a não serem vistos pelos administradores do sistema.

O papel principal dos rootkits é ocultar processos, ficheiros, logins e registos. Eles também podem interceptar dados dos terminais, ligações de rede ou periféricos, se eles incorporarem o software para tal.

Os rootkits não são maliciosos por natureza. Por exemplo, os sistemas e mesmo algumas aplicações ocultam ficheiros críticos usando rootkits. No entanto, eles são essencialmente utilizados para ocultar malware ou para esconder a presença de um intruso no sistema. Quando combinados com o malware, os rootkits são uma grande ameaça à integridade e segurança de um sistema. Eles podem monitorizar tráfego, criar backdoors no sistema, alterar ficheiros e relatórios e evitarem ser detectados.

Script

Outro termo para macro ou batch file, um script é uma lista de comandos que podem ser executados sem a interacção do utilizador.

Spam

Lixo de correio electrónico ou lixo de avisos de newsgroups. É normalmente conhecido como correio não-solicitado.

Spyware

O estabelecimento de ligação à Internet do utilizador sem o seu conhecimento, normalmente para propósitos de publicidade. As aplicações de spyware são tipicamente adicionadas como um elemento oculto de programas freeware ou shareware que podem ser download a partir da Internet; no entanto salientamos que a maioria das aplicações freeware ou shareware não possuem spyware. Uma vez instalado, o spyware monitoriza a actividade do utilizador na Internet e transmite essa informação em background para alguém. O spyware pode também reunir informação acerca de endereços de e-mail e até mesmo palavras-passe e números de cartões de crédito.

O spyware é similar a um cavalo-de-troia em que os utilizadores o instalam sem saberem, enquanto estão a instalar outra coisa qualquer. Uma forma comum de ser uma vítima de spyware é fazer download de determinado ficheiro peer-to-peer de produtos de swapping que se encontram actualmente disponíveis.

Para além destas questões de ética e privacidade, o spyware priva o utilizador de recursos de memória e também de largura de banda pois para enviar informação do utilizador para a fonte do spyware usa a ligação à Internet do utilizador. Por causa do spyware utilizar memória e recursos do sistema, as aplicações que estão a funcionar em background podem causar crashes no sistema ou uma grande instabilidade geral.

Itens no Startup

Qualquer ficheiro colocado nesta pasta, irá abrir quando o computador iniciar. Por exemplo, um ecrã que abra no ínicio, um ficheiro de som a ser tocado quando

ligar inicialmente o computador, um lembrete, ou programas de aplicação podem ser itens que começam a funcionar ao iniciar o computador. Normalmente, é colocado um pseudónimo deste ficheiro nesta pasta, em vez do ficheiro em si.

Área de notificação

Introduzido com o Windows 95, a área de notificação está localizada na barra de tarefas do Windows (normalmente em baixo junto ao relógio) e contém ícones em miniatura para um acesso fácil às funções do sistema tais como, fax, impressora, modem, volume, etc. Faça duplo-clique ou clique botão-direito sobre o ícone para ver e aceder aos detalhes e controlos.

TCP/IP

Transmission Control Protocol/Internet Protocol - Um conjunto de protocolos de uma rede de trabalho largamente usados na Internet e que permite comunicações ao londo de redes de computadores interconectadas com várias arquitecturas de hardware e vários sistemas operativos. O TCP/IP ínclui padrões de como os computadores comunicam e convenções para conectar redes e rotas de tráfego.

Trojan

Um programa destrutivo que se mascara de aplicação benigna. Ao contrário dos vírus, os cavalos de Tróia não se replicam, mas podem ser tão destrutivos como os vírus. Um dos cavalos de Tróia mais insidiosos é o programa que promete ver-se livre dos vírus do seu computador, mas em vez disso introduz vírus no seu computador.

O termo provém de uma história da Ilíada de Homero, na qual os Gregos deram um cavalo gigante de Madeira aos seus inimigos, os Troianos, como uma oferta majestosa. Mas após os Troianos levarem o cavalo para dentro das muralhas da sua cidade, os soldados Gregos saíram para fora do cavalo e abriram os portões da cidade, permitindo que os seus compatriotas entrassem e dominassem Tróia.

Actualização

Uma nova versão de um produto de software ou hardware desenhada para substituir uma versão antiga do mesmo produto. Em adição, a instalação de rotina da actualização verifica se a versão anterior já está instalada no seu computador; se não estiver, não poderá instalar a actualização.

O BitDefender tem o seu próprio módulo de actualização que lhe permite verificar actualizações manualmente, ou actualizar o produto automaticamente.

Vírus

Um programa ou um pedaço de código que é carregado no seu computador sem o seu conhecimento e executa-se contra a sua vontade. A maioria dos vírus podem-se replicar. Todos os vírus de computação são feitos pelo Homem. Um simples vírus que se possa reproduzir a si próprio vezes sem conta, é

relativamente fácil de fabricar. Mesmo um simples vírus é perigoso, porque usará rapidamente toda a memória disponível e levará o sistema a uma quebra. Um tipo de vírus ainda mais perigoso é aquele que é capaz de se transmitir ao longo das redes e ultrapassar sistemas de segurança.

assinatura de vírus

O padrão binário de um vírus, usado pelo programa antivírus para detectar e eliminar o vírus.

Worm

Um programa que se propaga a si próprio ao longo de uma rede, reproduzindo-se à medida que avança. Não pode ligar-se sozinho a outros programas.